MONOGRAPHIES
DE LA SOCIÉTÉ
MATHÉMATIQUE
DE FRANCE

3

G. KREISEL J. L. KRIVINE

ÉLÉMENTS DE LOGIQUE MATHÉMATIQUE

THÉORIE DES MODÈLES

DUNOD

MONOGRAPHIES DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE

3

G. KREISEL
Professeur
à l'Université de Stanford

J.L. KRIVINE
Maître assistant
à la Faculté des Sciences de Paris

ÉLÉMENTS DE LOGIQUE MATHÉMATIQUE

Théorie des modèles

DUNOD
PARIS
1967

AVANT-PROPOS

Ce livre expose les principes de la Méthode Axiomatique traitée, ici, dans son interprétation ensembliste, dite sémantique.

Les notions de base considérées sont : les différentes sortes de *langages*, les *réalisations* (types de structures mathématiques) qui leur sont associées et les *modèles* d'une formule (du langage) qui sont les réalisations satisfaisant à la formule. De là sont dérivées les notions de *conséquence* (une conclusion A étant la conséquence d'un ensemble d' « axiomes » $\mathscr{A}$ si tout modèle qui satisfait à chaque formule de $\mathscr{A}$ satisfait aussi à A) et de *définissabilité* (dans un modèle au moyen d'un langage donné).

Le langage qui permet le plus de résultats généraux est celui de la logique des prédicats du 1er ordre restreint à des formules finies. La plupart de ces résultats s'étendent à des formules infinies mais non pas à des langages d'ordre supérieur.

L'interprétation est ensembliste parce que les notions de base sont définies dans le vocabulaire de la théorie courante des ensembles (ensembles, relation d'appartenance et opérations logiques).

Ce livre contient les résultats élémentaires classiques sur ce sujet.

Le texte principal comprend 7 chapitres précédés d'un résumé.

L'Appendice I s'adresse aux lecteurs désireux d'examiner rapidement certaines applications mathématiques de la théorie générale de la méthode axiomatique, sans lire ou avant d'avoir lu le texte principal. La théorie non seulement conduit à des applications nouvelles ou, pour le moins, plus uniformes, de la méthode axiomatique (par exemple en Algèbre), mais aussi permet une formulation précise des idées qui ne jouent qu'un rôle heuristique dans la pratique courante.

L'Appendice II est destiné aux lecteurs possédant une certaine culture philosophique et intéressés par les problèmes des fondements des mathématiques. Les parties A et B esquissent les théories dites sémantiques et syntaxiques des fondements, y compris les théorèmes d'incomplétude de Gödel. Un lecteur qui, consciemment ou inconsciemment, serait influencé par les doctrines formalistes vulgarisées dans Bourbaki par exemple, ne pourrait se sentir à l'aise avec les notions de base de ces théories (ni devrait-il l'être avec la pratique mathématique s'il acceptait ces doctrines dans toutes leurs conséquences). L'introduction en soulignant, sans technicités, les faiblesses les plus évidentes de la position formaliste, aidera ce lecteur à aborder, l'esprit libre,

l'étude technique de ces notions. Les connaissances qu'il acquerra de la sorte lui permettront de faire une critique plus approfondie de la position (voir parties A et B in fine). On observera, dans la partie C, quelle que soit l'opinion que l'on se fasse de leur valeur respective, que l'analyse sémantique, loin d'être rendue périmée, est développée par l'analyse syntaxique. L'Appendice II peut être lu sans formation spécialisée en logique mathématique, sauf pour certains passages entre crochets ([ ]) qui se réfèrent à des problèmes philosophiques soulevés ou résolus par les théorèmes du texte principal.

Le texte est le développement de mon cours de Troisième Cycle à la Faculté des Sciences, Université de Paris, donné pour la première fois en 1960-61 et polycopié en 1962. Monsieur J. L. Krivine a rédigé les chapitres de 0 à 5, qui constituent une amélioration déterminante de mon exposé. J'ai mis le cours à jour en ajoutant les chapitres 6 et 7. Monsieur Lacombe qui m'a apporté son concours dans des domaines variés, a bien voulu traduire l'Appendice I et les résumés, et corriger mon français des chapitres 6 et 7. Monsieur J. P. Ressayre a traduit les parties A-C de l'Appendice II non sans avoir contribué à leur rédaction par ses questions et critiques.

Enfin, la collaboration efficace de mes amis Hubert Faure et Raymond Queneau mérite une mention particulière. Aux prises avec la traduction de plusieurs versions d'une longue introduction, ils m'ont amené, par leurs judicieuses remarques, à diviser le texte original en un avant-propos (H. F.) et une introduction à l'Appendice II (R. Q.). Ils ont eu en outre la délicatesse de dissiper mes scrupules de leur avoir fait perdre leur temps ; depuis nos tentatives initiales, le premier a doublé ses activités industrielles, le second a publié au moins un splendide roman.

G. KREISEL.

TABLE DES MATIÈRES

0. PRÉLIMINAIRES : SCHÉMAS FONCTIONNELS

Résumé

Ce chapitre contient des résultats élémentaires sur les classes de fonctions engendrées par des schémas finis. De tels schémas sont fréquemment utilisés en mathématiques (polynômes sur un anneau quelconque, fractions rationnelles sur un corps quelconque, ...) ; ici, ils sont principalement appliqués à la construction de langages. Le théorème de la page 2 établit l'existence des notations dites « sans parenthèses ».

Toutes les définitions sont exprimées à partir des notions de base de la théorie des ensembles (héréditairement finis). On utilisera ce fait dans l'Appendice II.

On se donne une famille dénombrable F_n ($n = 0, 1, \ldots$) d'ensembles disjoints. Un élément de F_n sera appelé symbole fonctionnel à n variables.

Posons $F = \bigcup_n F_n$ et désignons par $\sigma(F)$ l'ensemble des suites finies d'éléments de F. (Une suite finie d'éléments de F soit $(f_1, f_2, \ldots, f_k)$ par exemple, sera notée plus brièvement $f_1\, f_2 \ldots f_k$). Considérons les sous-ensembles M de $\sigma(F)$ ayant la propriété suivante :

Si $a_1, \ldots, a_n$ sont des éléments de M et si $f \in F_n$, alors $fa_1 \ldots a_n \in M$ (nous désignerons cette propriété par « propriété S »).

Toute intersection d'ensembles ayant la propriété S a encore cette propriété. Par suite l'intersection de tous les sous-ensembles de $\sigma(F)$ ayant cette propriété la possède aussi. Cette intersection est appelée clôture fonctionnelle de la famille (F_n) et sera désignée par $\overline{F}$. Un élément de $\overline{F}$ est appelé schéma fonctionnel (construit à l'aide des symboles de F).

Pour que $\overline{F}$ *soit non vide il faut et il suffit que* $F_0 \neq \phi$ (c'est-à-dire qu'il existe des symboles fonctionnels à 0 variables appelés encore symboles de constantes). En effet, si F_0 est non vide, soit $a \in F_0$. Alors a est dans tous les ensembles ayant la propriété S, donc $a \in \overline{F}$. Inversement si F_0 est vide, ϕ a la propriété S donc $\overline{F} = \phi$.

Tout élément de $\overline{F}$ *est de la forme* $fa_1 \dots a_n$ *avec* $f \in F_n$ *et* $a_1, \dots, a_n \in \overline{F}$. En effet soit E l'ensemble des éléments de cette forme ; $\overline{F}$ ayant la propriété S, il est évident que tout élément de E est dans $\overline{F}$. Inversement comme E a aussi la propriété S, $E \supset \overline{F}$. C. q. f. d.

Si $x \in \sigma(F)$ et $a \in F$ on appelle occurrence de a dans x la donnée de deux suites u, $v \in \sigma(F)$ (éventuellement vides), telles que $x = uav$. Si $y \in \sigma(F)$, la suite uyv est dite « obtenue en remplaçant par y l'occurence considérée de a dans x ».

Si x et y sont des schémas fonctionnels ($x, y \in \overline{F}$) et si $a \in F_0$, la suite z obtenue en remplaçant une occurrence de a dans x par y est aussi un schéma fonctionnel.

Démonstration par récurrence sur la longueur de x : si x est de longueur 1, ou bien $x = a$ et $z = y$, ou bien $x \neq a$ et $z = x$; dans les deux cas $z \in \overline{F}$. Si x est de longueur $n > 1$, on a $x = fu_1 \dots u_k$, avec $f \in F_k$, $u_1, \dots, u_k$ étant des schémas fonctionnels de longueur $< n$. L'un d'eux, soit u_i (avec $1 \leqslant i \leqslant k$) contient l'occurrence considérée de a. Soit v_i la suite obtenue en remplaçant cette occurrence par y dans u_i. Alors $v_i \in \overline{F}$ d'après l'hypothèse de récurrence. Or

$$z = fu_1 \dots u_{i-1}\, v_i\, u_{i+1} \dots u_k ,$$

donc $z \in \overline{F}$.

C. q. f. d.

LEMME. — *Si $a \in \overline{F}$ et si $u \in \sigma(F)$, $u \neq \phi$, alors $au \notin \overline{F}$.*

Par récurrence sur la longueur de a. Si a est de longueur 1 on a $a \in F_0$. Si au était dans $\overline{F}$ on aurait $au = fa_1 \dots a_k$ avec $f \in F_k$ et $a_1, \dots, a_k \in \overline{F}$. D'où $f = a$ (premier symbole de chaque membre) et par suite $k = 0$. D'où $au = a$ et $u = \phi$.

Supposons le lemme vrai pour tous les éléments de $\overline{F}$ de longueur $< n$ et soit $a \in \overline{F}$, a étant de longueur n. On a $a = fa_1 \dots a_k$ avec $f \in F_k$ et $a_1, \dots, a_k \in \overline{F}$. Si $au \in \overline{F}$ on a $au = gb_1 \dots b_l$ avec $g \in F_l$ et $b_1, \dots, b_l \in \overline{F}$. D'où $fa_1 \dots a_k u = gb_1 \dots b_l$; et par suite $f = g$. Soit i le plus petit entier tel que $a_i \neq b_i$. On a donc

$$a_i\, a_{i+1} \dots a_k\, u = b_i\, b_{i+1} \dots b_l$$

et par suite on a soit $a_i = b_i\, v$, soit $a_i\, v = b_i$ avec $v \in \sigma(F)$ et $v \neq \phi$. Or cela contredit l'hypothèse de récurrence. (L'égalité $a_i = b_i\, v$ entraînant que la longueur de b_i est $< n$.)

THÉORÈME. — *Pour tout $x \in \overline{F}$ il y a une façon et une seule d'écrire x sous la forme $fa_1 \dots a_n$ avec $f \in F_n$ et $a_1, \dots, a_n \in \overline{F}$.*

S'il existait deux telles façons d'écrire x, on aurait $fa_1 \dots a_n = gb_1 \dots b_p$ avec $f \in F_n$, $g \in F_p$, $a_1, \dots, a_n$, $b_1, \dots, b_p \in \overline{F}$. On a alors $f = g$. En désignant

par i le plus petit entier tel que $a_i \neq b_i$, on obtient $a_i \ldots a_n = b_i \ldots b_p$ et par suite $a_i = b_i v$ ou $a_i v = b_i$ ce qui contredit le lemme précédent.

Le théorème suivant sera très utilisé dans la suite :

THÉORÈME. — *Etant donnés un ensemble X, et, pour chaque n, une application $f \to \hat{f}$ de F_n dans l'ensemble des applications de X^n dans X, il existe une application $x \to \bar{x}$ de $\bar{F}$ dans X, et une seule, telle que pour tout $f \in F_n$ et pour tout $a_1, \ldots, a_n \in \bar{F}$ on ait*

$$\overline{fa_1 \ldots a_n} = \hat{f}(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n) .$$

Unicité : étant données deux telles applications l'ensemble U des éléments de $\bar{F}$ sur lesquels elles coïncident à la propriété S. Donc $U \supset \bar{F}$ et par suite $U = \bar{F}$.

Existence : désignons par Φ_n le sous-ensemble de $\bar{F}$ formé des éléments de longueur n. On définit par récurrence sur n une application φ_n de Φ_n dans X de la façon suivante : pour $n = 1$, comme $\Phi_1 = F_0$, pour tout $x \in \Phi_1$ on pose $\varphi_1(x) = \hat{x}$. Supposons définie φ_i pour $i < n$. Si $x \in \Phi_n$, on a d'une seule façon $x = fa_1 \ldots a_k$ avec $f \in F_k$, et $a_i \in \bar{F}$ de longueur $l_i < n$. On pose alors

$$\varphi_n(x) = \hat{f}\left(\varphi_{l_1}(a_1), \varphi_{l_2}(a_2), \ldots, \varphi_{l_k}(a_k)\right) .$$

L'application cherchée $x \to \bar{x}$ est alors donnée par $\bar{x} = \varphi_n(x)$ si x est de longueur n. Il est immédiat qu'elle satisfait à la condition imposée.

Cas particulier : chaque $f \in F_n$ définit une fonction $\hat{f}$ à n variables sur $\bar{F}$: si $a_1, \ldots, a_n \in \bar{F}$ on pose $\hat{f}(a_1, \ldots, a_n) = fa_1 \ldots a_n$. Cette fonction $\hat{f}$ sera appelée *valeur naturelle* de f sur la clôture fonctionnelle de F.

---

1. CALCUL PROPOSITIONNEL

Résumé

Les notions traitées dans ce chapitre concernent les connecteurs grammaticaux, par exemple la négation, la conjonction, la disjonction. Ces opérations permettent de composer des propositions à partir de propositions données. Les connecteurs particuliers qui sont traités ici sont appelés « aristotéliciens », « classiques », ou encore « bivalents », parce qu'ils ont été mis en évidence par Aristote, et parce qu'ils sont destinés à être appliqués à des propositions à valeur bien définie (vraie ou fausse) et non pas indécidée. De plus, les connecteurs étudiés doivent dépendre seulement de la valeur de vérité prise par chacune des propositions auxquelles on les applique ; cette condition n'est pas satisfaite lorsqu'on prend, par exemple l'une des significations usuelle de l'implication (A implique B) où l'on suppose que l'hypothèse A a « quelque chose à voir » avec la conclusion B.

La structure constituée par les connecteurs étudiés ici (qui sont appelés « fonctions de vérité ») est celle de la classe de toutes les applications de $\{0,1\}^n$ dans $\{0,1\}$. L'exercice 1 indique de façon précise en quel sens l'ensemble de tous ces connecteurs peut être obtenu par superposition à partir des connecteurs particuliers indiqués dans le texte. Comme la structure en question est très simple, le seul problème mathématiquement intéressant est celui des ensembles *infinis* de formules propositionnelles.

Les notions de base sont celles de « formule propositionnelle » (dont la définition utilise le contenu du chapitre précédent) et de « modèle » d'un ensemble quelconque de formules. La seconde notion constitue un cas particulier de la notion générale de modèle en logique des prédicats. Le principal résultat est le théorème de finitude, qui se démontre par une simple utilisation de la compacité. Certaines applications algébriques sont données dans les exercices 3 et 4.

Etant donné un ensemble P on appelle « calcul propositionnel construit à l'aide des éléments de P » et on désigne par Prop(P) l'ensemble des schémas fonctionnels construits à l'aide des symboles suivants :

1) les symboles fonctionnels à 0 variable sont $\top$, $\bot$ et les éléments de P. ($\top$ se lit « vrai », $\bot$ se lit « faux »),
2) $\neg$ est le seul symbole à 1 variable (il se lit « non »),
3) $\vee$ est le seul symbole à 2 variables (il se lit « ou »).

Les éléments de P sont appelés variables propositionnelles ; les éléments de $\mathrm{Prop}(P)$ sont appelés formules.

Pour $A, B \in \mathrm{Prop}(P)$, $\vee AB$ sera souvent notée $(A) \vee (B)$; $\neg((\neg A) \vee (\neg B))$ sera notée $(A) \wedge (B)$ (le signe $\wedge$ se lisant « et ») ; $(\neg A) \vee (B)$ sera notée $(A) \rightarrow (B)$ (le signe $\rightarrow$ se lisant « implique »). $(A \rightarrow B) \wedge (B \rightarrow A)$ sera notée $(A) \leftrightarrow (B)$ (le signe $\leftrightarrow$ se lisant « équivaut à »). Pour faciliter la lecture, on supprimera parfois les parenthèses, s'il n'y a pas de confusion possible, et on utilisera aussi des crochets : par exemple $[(A) \rightarrow (B)]$ à la place de $((A) \rightarrow (B))$.

On appelle *réalisation* du calcul propositionnel construit sur P toute application δ de P dans $\{0, 1\}$ (ou plus généralement dans un ensemble ordonné à 2 éléments).

D'après le théorème fondamental sur les schémas fonctionnels, *toute réalisation δ se prolonge en une application (notée aussi δ) de* $\mathrm{Prop}(P)$ *dans* $\{0, 1\}$, si on donne à $\top$ la valeur 1, à $\bot$ la valeur 0, et à $\neg$ et $\vee$ les valeurs suivantes (fonctions à valeurs dans $\{0, 1\}$, définies sur $\{0, 1\}$ et $\{0, 1\}^2$) : $\neg 0 = 1$; $\neg 1 = 0$; $\vee 00 = 0$; $\vee 10 = \vee 01 = \vee 11 = 1$. On dit qu'une réalisation δ de $\mathrm{Prop}(P)$ satisfait une formule $A \in \mathrm{Prop}(P)$ ou est un modèle de A si $\delta(A) = 1$.

On dit qu'une réalisation δ satisfait un ensemble $\mathscr{A}$ de formules, ou est un modèle de $\mathscr{A}$ si δ satisfait chaque formule de $\mathscr{A}$.

Une formule $A \in \mathrm{Prop}(P)$ est appelée « théorème du calcul propositionnel » ou « formule valide du calcul propositionnel » si toute réalisation la satisfait. Deux formules A et B sont dites équivalentes si $A \leftrightarrow B$ est un théorème, ou si $\delta(A) = \delta(B)$ dans toute réalisation (ce qui revient évidemment au même).

LEMME D'INTERPOLATION. — *Si $A \vee B$ est un théorème de* $\mathrm{Prop}(P)$, *il existe une formule C dont toutes les variables propositionnelles sont communes à A et B et telle que $A \vee C$ et $\neg C \vee B$ soient des théorèmes de* $\mathrm{Prop}(P)$.

Par récurrence sur le nombre k de variables propositionnelles qui sont dans A sans être dans B. Si $k = 0$ il suffit de poser $C = \neg A$; supposons le lemme démontré pour $k = n - 1$ et soit A une formule telle que $A \vee B$ soit un théorème et qui ait exactement n variables propositionnelles qui ne soient pas dans B. Soit p l'une de ces variables, soient A_1 et A_2 les formules obtenues en substituant $\top$ et $\bot$ à p dans A. $A_1 \vee B$ et $A_2 \vee B$ sont des théorèmes, donc $(A_1 \wedge A_2) \vee B$ est un théorème auquel on peut appliquer l'hypothèse de récurrence. On obtient ainsi une formule C telle que $(A_1 \wedge A_2) \vee C$ et $(\neg C) \vee B$ soient des théorèmes. De la définition de A_1 et A_2 il résulte que $A \vee C$ est un théorème. C. q. f. d.

En remplaçant A par $\neg A$ on obtient l'énoncé suivant :

Si $A \rightarrow B$ est un théorème de $\mathrm{Prop}(P)$ *il existe une formule C dont les variables propositionnelles sont communes à A et B et telle que $A \rightarrow C$ et $C \rightarrow B$ soient deux théorèmes.*

COROLLAIRE. — THÉORÈME DE DÉFINISSABILITÉ. *Soient $A(p)$ une formule contenant la variable propositionnelle p, et $A(p')$ le résultat de la substitution de p' à p dans $A(p)$ (p' étant une variable propositionnelle qui n'est pas dans $A(p)$). Si $[A(p) \wedge A(p')] \to (p \to p')$ est un théorème, il existe une formule F ne contenant que les variables de A mais ni p ni p' telle que $A(p) \to (p \leftrightarrow F)$ soit un théorème.*

En effet $A(p) \wedge p \wedge A(p') \to p'$ est un théorème donc $A(p) \wedge p \to (A(p') \to p')$ est un théorème. D'après le lemme d'interpolation on a donc une formule F ne contenant ni p ni p' telle que $A(p) \wedge p \to F$ et $F \to (A(p') \to p')$ soient des théorèmes. Donc $A(p) \to (p \to F)$ et $A(p') \to (F \to p')$ sont des théorèmes et par suite $A(p) \to (p \leftrightarrow F)$ est un théorème.

Plus explicitement, $F = A(\top)$ (résultat de la substitution de $\top$ à p dans $A(p)$).

Démonstration. — En remplaçant $A(p) \wedge p \to (A(p') \to p')$ par

$$(\neg\ A(p) \vee \neg p) \vee (A(p') \to p')$$

on obtient d'après la démonstration du lemme d'interpolation

$$F = \neg\ ((\neg\ A(\top) \vee \bot) \wedge (\neg\ A(\bot) \vee \top))$$

qui se réduit à $\neg\ \neg\ A(\top)$ d'où $F = A(\top)$.

Le théorème suivant sera utilisé pour l'élimination des quantificateurs (Chapitre 4).

THÉORÈME. — *Toute formule A de* Prop(P) *est équivalente à une formule de la forme $A_1 \vee A_2 \vee \cdots \vee A_k$, où chaque A_i $(1 \leqslant i \leqslant k)$ est de la forme $A_i = \alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_r$, avec $\alpha = p$ ou $\neg p$, où p est une variable propositionnelle de A ou $\top$.*

On dit qu'on a écrit A sous la forme d'une « disjonction de conjonctions ». Le théorème est également vrai pour une « conjonction de disjonctions » et se démontre de la même façon.

Par récurrence sur le nombre k de variables propositionnelles apparaissant dans A. Pour $k = 0$, A équivaut soit à $\top$ soit à $\bot$. Supposons le théorème démontré pour $k = n - 1$, et soit $A(p)$ une formule contenant n variables propositionnelles, dont p. Soient B et C les résultats de la substitution de $\top$ et de $\bot$ à p dans $A(p)$. B et C ont $n - 1$ variables propositionnelles et il est immédiat que $A(p)$ équivaut à $(p \wedge B) \vee (\neg p \wedge C)$. D'après l'hypothèse de récurrence B équivaut à $B_1 \vee \cdots \vee B_k$ et C équivaut à $C_1 \vee \cdots \vee C_l$, donc $A(p)$ équivaut à

$$(p \wedge B_1) \vee (p \wedge B_2) \vee \cdots \vee (p \wedge B_k) \vee (\neg p \wedge C_1) \vee \cdots \vee (\neg p \wedge C_l),$$

qui est de la forme cherchée. C. q. f. d.

THÉORÈME DE FINITUDE. — *Soit* $\mathscr{A}$ *un ensemble de formules de* Prop(P) *tel que tout sous-ensemble fini ait un modèle. Alors* $\mathscr{A}$ *a un modèle.*

Démontrons-le d'abord dans le cas (le plus courant en logique) où P est dénombrable (et par suite aussi $\mathscr{A}$).

Soit $p_1, ..., p_k, ...$ une énumération de P. Supposons trouvée une application δ de $\{ p_1, ..., p_n \}$ dans $\{ 0, 1 \}$ telle que tout sous-ensemble fini de $\mathscr{A}$ ait un modèle dans lequel $p_1, ..., p_n$ prennent les valeurs $\delta(p_1), ..., \delta(p_n)$. Alors on peut prolonger δ à $\{ p_1, ..., p_n, p_{n+1} \}$ avec la même propriété. En effet si $\delta(p_{n+1}) = 0$ ne convient pas, c'est qu'il existe un sous-ensemble fini U_0 de $\mathscr{A}$ qui ne peut être satisfait quand $p_1, ..., p_n, p_{n+1}$ prennent les valeurs $\delta(p_1), ..., \delta(p_n), 0$. Si U est un sous-ensemble fini quelconque de $\mathscr{A}$, d'après l'hypothèse faite sur δ, $U_0 \cup U$ a un modèle dans lequel $p_1, ..., p_n$ prennent les valeurs $\delta(p_1), ..., \delta(p_n)$. Dans ce modèle p_{n+1} prend donc la valeur 1 et par suite tout sous-ensemble fini U de $\mathscr{A}$ à un modèle dans lequel $p_1, ..., p_n, p_{n+1}$ prennent les valeurs respectives $\delta(p_1), .., \delta(p_n), 1$.

On définit donc ainsi par récurrence sur n une réalisation δ de Prop(P), telle que, pour chaque n, tout sous-ensemble fini de $\mathscr{A}$ ait un modèle dans lequel $p_1, ..., p_n$ prennent les valeurs $\delta(p_1) ... \delta(p_n)$. Il en résulte que δ satisfait $\mathscr{A}$: si A est une formule de $\mathscr{A}$, il suffit pour voir que δ satisfait A, de prendre n assez grand pour que les variables propositionnelles de A forment un sous-ensemble de $\{ p_1, ..., p_n \}$.

Cette démonstration est valable dans le cas général, moyennant un bon ordre sur P. On peut aussi donner la démonstration suivante :

Pour chaque formule A de Prop (P) l'ensemble des réalisations δ qui la satisfont est ouvert dans $\{ 0, 1 \}^P$ (muni de la topologie produit) puisque A ne fait intervenir qu'un nombre fini de variables propositionnelles. Il est également fermé puisque les réalisations qui ne satisfont pas A sont celles qui satisfont $\neg A$. Pour chaque formule A de $\mathscr{A}$ soit $\bar{A}$ l'ensemble des réalisations qui satisfont A. L'hypothèse du théorème entraîne que toute intersection finie de $\bar{A}$ est non vide. Comme $\{ 0, 1 \}^P$ est compact, l'intersection de tous les $\bar{A}$ pour $A \in \mathscr{A}$ est donc non vide. C. q. f. d.

AUTRE ÉNONCÉ. — *Si toute réalisation satisfait une des formules d'un ensemble* $\mathscr{B}$ *de formules, il existe* $B_1, ..., B_n \in \mathscr{B}$ *telles que* $B_1 \vee \cdots \vee B_n$ *soit un théorème.*

Sinon pour tout sous-ensemble fini $\{ B_1, ..., B_n \}$ de $\mathscr{B}$ il y a une réalisation qui ne satisfait pas $B_1 \vee \cdots \vee B_n$ donc qui satisfait $\neg B_1 \wedge \cdots \wedge \neg B_n$. Soit $\mathscr{A}$ l'ensemble des $\neg B$ pour $B \in \mathscr{B}$. D'après le théorème de finitude il y a une réalisation qui satisfait $\mathscr{A}$ ce qui contredit l'hypothèse.

On dit qu'une formule A est *conséquence d'un ensemble* $\mathscr{A}$ *de formules* si toute réalisation qui satisfait $\mathscr{A}$ satisfait également A. En particulier les conséquences de ϕ sont les théorèmes ; les conséquences d'un ensemble fini

$\mathscr{A} = \{ A_1, ..., A_n \}$ sont les formules A telles que $A_1 \wedge \cdots \wedge A_n \to A$ soit un théorème.

THÉORÈME. — *Pour que A soit conséquence d'un ensemble $\mathscr{A}$ de formules, il faut et il suffit qu'elle soit conséquence d'un sous-ensemble fini de $\mathscr{A}$.*

La condition est évidemment suffisante. Elle est nécessaire, car dire que A est conséquence de $\mathscr{A}$ équivaut à dire que l'ensemble $\mathscr{A} \cup \{ \neg A \}$ n'a pas de modèle. Il y a donc un sous-ensemble fini $\{ A_1, ..., A_n, \neg A \}$ qui n'a pas de modèle (si $\neg A$ n'est pas dans ce sous-ensemble, il suffit de l'y ajouter).

C. q. f. d.

EXERCICES

1. Il est immédiat que chaque formule A ayant $p_1, ..., p_n$, comme variables propositionnelles définit une application de $\{ 0, 1 \}^n$ dans $\{ 0, 1 \}$. Démontrer que toute application de $\{ 0, 1 \}^n$ dans $\{ 0, 1 \}$ est ainsi obtenue.

Soit U_k l'ensemble des applications de $\{ 0, 1 \}^k$ dans $\{ 0, 1 \}$ et $U = \bigcup_{k \in N} U_k$. Un sous-ensemble S de U est dit complet si tout élément de U s'obtient par composition d'éléments de S.

Montrer que les ensembles $S = \{ \varphi \}$, $S = \{ \to, \bot \}$ sont complets (où $\varphi(p, q) = \neg p \wedge \neg q$). Montrer que les ensembles $S = \{ \top, \to \}$, $S = \{ \top, \to, \wedge, \vee \}$ ne sont pas complets.

Solution. — Par récurrence sur le nombre n de variables. Supposons la proposition démontrée pour $n = k$ et soit $f(p_1, ..., p_k, p_{k+1})$ une application de $\{ 0, 1 \}^{k+1}$ dans $\{ 0, 1 \}$. Par hypothèse on a

$$f(p_1, ..., p_k, 1) = A(p_1, ..., p_k)$$

et $f(p_1, ..., p_k, 0) = B(p_1, ..., p_k)$, A et B étant deux formules dont les variables sont $p_1, ..., p_k$. On vérifie immédiatement que la fonction $f(p_1, ..., p_k, p_{k+1})$ est donnée par la formule

$$[p_{k+1} \to A(p_1, ..., p_k)] \wedge [\neg p_{k+1} \to B(p_1, ..., p_k)] .$$

On vient de montrer que l'ensemble $\{ \neg, \vee \}$ est complet. Or $\neg p = \varphi(p, p) = p \to \bot$ et $p \vee q = \neg \varphi(p, q) = \neg p \to q$, ce qui montre que les ensembles $\{ \varphi \}$ et $\{ \to, \bot \}$ sont complets.

Considérons les schémas fonctionnels construits à l'aide de $\{ \top, \to \}$ et d'un ensemble P de variables propositionnelles. Ils représentent toutes les fonctions obtenues à partir de $\top$, $\to$ par composition. Soit $A(p)$ un schéma fonctionnel ne contenant que la variable p. On va voir par

récurrence sur la longueur que $A(p) \leftrightarrow \top$ ou bien $A(p) \leftrightarrow p$ est un théorème. Si $A(p)$ est de longueur n on a $A(p) = \rightarrow B(p)\, C(p)$, où $B(p)$ et $C(p)$ sont de longueur $\leqslant n - 1$. Il en résulte que $A(p)$ équivaut à une des formules $p \rightarrow p$, $p \rightarrow \top$, $\top \rightarrow p$, $\top \rightarrow \top$, c'est-à-dire à $\top$ ou à p.

Il en résulte que la fonction $\neg$ n'est pas obtenue par composition de $\top$ et de $\rightarrow$. On montrera de même qu'elle n'est pas obtenue par composition de $\top$, $\rightarrow$, $\wedge$, $\vee$.

2. Un ensemble $\mathscr{A}$ de formules est dit indépendant si aucune formule $A \in \mathscr{A}$ n'est conséquence de $\mathscr{A} - \{ A \}$. Démontrer que :

a) Pour qu'un ensemble $\mathscr{A}$ de formules soit indépendant, il faut et il suffit que tout sous-ensemble fini le soit.

b) Pour tout ensemble $\mathscr{A}$ fini, il y a un sous-ensemble indépendant équivalent $\mathscr{B}$ (c'est-à-dire tel que toute formule de $\mathscr{A}$ soit conséquence de $\mathscr{B}$ et inversement).

c) Pour tout ensemble $\mathscr{A}$ dénombrable il existe un ensemble indépendant équivalent.

Remarque. — Il existe un ensemble dénombrable $\mathscr{A}$ de formules qui n'a aucun sous-ensemble indépendant équivalent à $\mathscr{A}$. Désignons par $p_1, ..., p_n ...$ une suite de variables propositionnelles distinctes et posons par exemple :

$$\mathscr{A} = (p_1, p_1 \wedge p_2, ..., p_1 \wedge \cdots \wedge p_n, ...) .$$

Il est clair que tout sous-ensemble indépendant de $\mathscr{A}$ est réduit à une seule formule et que $\mathscr{A}$ n'est équivalent à aucun de ses éléments.

Solution. — *a*) Conséquence immédiate du théorème de finitude.

b) Par récurrence sur le nombre k d'éléments de $\mathscr{A}$.

La proposition est évidente pour $k = 0$: supposons-la vraie pour $k = n$ et soit $\mathscr{A} = \{ A_1, ..., A_n, A_{n+1} \}$ un ensemble de $n + 1$ formules. Si cet ensemble est indépendant la proposition est vraie. Sinon A_{n+1} par exemple est conséquence de $\{ A_1, ..., A_n \}$ et il suffit alors d'appliquer l'hypothèse de récurrence à l'ensemble $\{ A_1, ..., A_n \}$.

c) Soit $A_1, ..., A_n, ...$ une énumération des formules de $\mathscr{A}$. Soit A_i la première formule dans cette énumération qui ne soit pas un théorème. Posons $B_1 = A_i$ et par récurrence posons $B_{n+1} = B_n \wedge A_j$ où A_j est la première formule de $\mathscr{A}$ qui ne soit pas conséquence de B_n. Il est immédiat que $B_1, B_2, ..., B_n, ...$ sont conséquences de $\mathscr{A}$ et qu'inversement chaque A_n est conséquence de l'ensemble $B_1, ..., B_n, ...$. Dans la suite $B_1, ..., B_n, ...$ chaque formule est conséquence de la suivante, mais non

de la précédente. Si cette suite est finie, soit B_n son dernier terme. $\{ B_n \}$ est l'ensemble indépendant cherché (il est indépendant car si B_n était un théorème, comme $B_n \to B_1$ en est un, B_1 serait aussi un théorème).

Si cette suite est infinie, posons $C_1 = B_1$; $C_2 = B_1 \to B_2$; ... ; $C_n = B_{n-1} \to B_n$; il est immédiat que 1° aucune C_n n'est un théorème et 2° l'ensemble $\{ C_1, C_2, ..., C_n, ... \}$ est équivalent à $\mathscr{A}$. Il est indépendant : en effet d'après le 1°, il y a une réalisation qui satisfait $\neg C_n$ et donc B_{n-1} et $\neg B_n$. Comme $\neg B_n \to \neg B_m$, pour $m \geqslant n$, cette réalisation satisfait C_m, $m > n$; comme $B_n \to B_p$, pour $p \leqslant n$, elle satisfait C_p, pour $p < n$. Alors elle satisfait toutes les formules C_q, $q \neq n$, et ne satisfait pas C_n, c'est-à-dire C_n n'est pas conséquence de $\{ C_1, ..., C_{n-1}, C_{n+1}, ... \}$.

C. q. f. d.

3. *a*) Un groupe G est dit totalement ordonné si on a sur G une relation d'ordre total telle que $a \leqslant b \Rightarrow ac \leqslant bc$ et $ca \leqslant cb$ quels que soient $a, b, c \in G$. Montrer que pour qu'un groupe G puisse être ordonné il faut et il suffit que tout sous-groupe de G engendré par un ensemble fini d'éléments de G puisse être ordonné.

b) En déduire que pour qu'un groupe commutatif G puisse être ordonné il faut et il suffit qu'il soit sans torsion.

Solution. — *a*) La condition est évidemment nécessaire. Considérons alors dans le calcul propositionnel construit avec les éléments de G^2 comme variables propositionnelles l'ensemble $\mathscr{A}$ des formules suivantes :

(a, a), où a décrit G.
$(a, b) \vee (b, a)$, où a et b décrivent G.
$(a, b) \to \neg (b, a)$, où a, b décrivent G en restant distincts.
$(a, b) \wedge (b, c) \to (a, c)$, où a, b, c décrivent G.
$(a, b) \to [(ac, bc) \wedge (ca, cb)]$, où a, b, c décrivent G.

Dans tout sous-ensemble fini de $\mathscr{A}$, soit U, n'apparaissent qu'un nombre fini d'éléments de G. Si G_U est le sous-groupe qu'ils engendrent, G_U peut être ordonné ce qui revient à dire qu'il existe une réalisation du calcul propositionnel considéré qui satisfait U : celle qui donne à (a, b) la valeur 1 ou 0 suivant que $a < b$ ou $a \geqslant b$ pour $a, b \in G_U$, et une valeur arbitraire si a ou b n'est pas dans G_U. D'après le théorème de finitude, il y a une réalisation qui satisfait $\mathscr{A}$ tout entier. Il suffit de poser $a < b$ quand $(a, b) = 1$ dans cette réalisation et $a \geqslant b$ quand $(a, b) = 0$ pour obtenir un ordre sur G.

b) Si G est commutatif et ordonné il est clair que G est sans torsion. Inversement si G est sans torsion, les sous-groupes de G engendrés par un nombre fini d'éléments sont libres donc isomorphes à $\mathbf{Z}^n$ pour un

entier n. Or $\mathbf{Z}^n$ peut être ordonné suivant l'ordre lexicographique : $(a_1, ..., a_n) < (b_1, ..., b_n)$ si et seulement si pour le premier i tel que $a_i \neq b_i$ on a $a_i < b_i$.

4. Un graphe (relation symétrique et non réflexive) défini sur un ensemble M est dit k-chromatique (k étant un entier positif) s'il existe une partition de M en k ensembles disjoints $C_1, ..., C_k$, tels que deux éléments de M liés par le graphe n'appartiennent pas au même C_i. Montrer que pour qu'un graphe soit k-chromatique, il faut et il suffit que chaque sous-graphe fini le soit.

Solution. — La condition est évidemment nécessaire, une partition sur M induisant une partition sur chaque sous-ensemble fini. Inversement considérons dans le calcul propositionnel construit sur $\{1, 2, ..., k\} \times M$ comme ensemble de variables propositionnelles, l'ensemble $\mathscr{A}$ des formules suivantes :

$(i, a) \rightarrow \neg (j, a)$, où i, j sont deux entiers distincts et $\leqslant k$ et où a décrit M ;
$(1, a) \vee (2, a) \vee \cdots \vee (k, a)$, où a décrit M ;
$(i, a) \rightarrow \neg (i, b)$, où $i \leqslant k$ et où a, b sont deux éléments liés.

Si tout sous-graphe fini est k-chromatique on voit immédiatement que tout sous-ensemble fini de $\mathscr{A}$ a un modèle. Donc $\mathscr{A}$ tout entier a un modèle. On obtient sur M une partition k-chromatique en posant $a \in C_i$ si et seulement si (i, a) prend la valeur 1 dans ce modèle.

---

2. CALCUL DES PRÉDICATS

Résumé

On élargit l'étude effectuée au chapitre précédent, en prenant maintenant en considération les quantificateurs « quel que soit » et « il existe ». Ces quantificateurs n'opèrent pas sur les propositions mais sur les relations, permettant de définir des relations n-aires à partir de relations $(n + 1)$-aires, et en particulier des propositions (relations 0-aires) à partir de relations monadiques. Corrélativement, on élargit l'emploi des connecteurs propositionnels définis dans le chapitre précédent, de façon à les transformer eux aussi en des opérations portant sur les relations.

Le langage obtenu se révèle suffisant pour exprimer la majorité des concepts mathématiques, et constitue par conséquent un cadre adéquat pour une théorie générale des systèmes axiomatiques.

Contrairement à ce qui se passe pour le calcul propositionnel, lorsqu'on définit comme ci-dessus la notion générale de « quantificateur », il n'est pas vrai que tous les quantificateurs puissent être définis à partir des deux quantificateurs particuliers indiqués ci-dessus. Pour plus de détails, cf. Mostowski [FM], **44** (1957).

Les principales notions sont celles de « formule » ou de « langage » de la logique des prédicats (du premier ordre), et celle de « réalisation » d'un langage. A partir de ces notions, on définit celle de « modèle » d'un ensemble de formules. Un cas particulier important est celui des modèles qu'on appelle « canoniques », c'est-à-dire ceux où chaque objet (élément du modèle) possède un *nom* dans le langage considéré.

Dans ce chapitre, le principal outil est constitué par l'emploi de schémas fonctionnels pour la construction de modèles canoniques. Par cette méthode on obtient en particulier les résultats suivants : on construit, pour tout modèle d'un ensemble fini ou dénombrable quelconque de formules, des *sous*-modèles dénombrables de ce modèle (exercice 5) ; on démontre un certain théorème de finitude (par réduction au cas propositionnel) ; on obtient un utile théorème d'uniformité. L'exercice 6 montre que ce dernier théorème est optimal à plusieurs points de vue.

D'autres résultats concernant les principales questions de ce chapitre seront donnés dans les chapitres 3 et 5. Ce dernier contient une seconde méthode pour construire des modèles canoniques (et une seconde démonstration des principaux résultats du présent chapitre).

Les méthodes de ce chapitre se prêtent à une démonstration du théorème d'interpolation : on la donne donc ici ; mais l'intérêt de ce théorème est lié aux problèmes de définissabilité traités systématiquement dans les chapitres 4 et 6.

UN LANGAGE $\mathscr{L}$ est par définition constitué par :

1° *Un ensemble* $V_{\mathscr{L}}$ dont les éléments sont appelés variables.

2° *Une suite d'ensembles* $F^n_{\mathscr{L}}(n = 0, 1, ...)$. Les éléments de $F^n_{\mathscr{L}}$ sont appelés symboles fonctionnels à n variables. On pose $F_{\mathscr{L}} = \bigcup_n F^n_{\mathscr{L}}$. $F_{\mathscr{L}}$ est appelé ensemble des symboles fonctionnels.

3° *Une suite d'ensembles* $R^n_{\mathscr{L}}$ $(n = 0, 1, ...)$. Les éléments de $R^n_{\mathscr{L}}$ sont appelés symboles relationnels à n variables.

Les ensembles $V_{\mathscr{L}}$, $R^n_{\mathscr{L}}$, $F^n_{\mathscr{L}}$ sont supposés de plus disjoints deux à deux.

On appelle ensemble des termes de $\mathscr{L}$ *et on désigne par* $T_{\mathscr{L}}$ l'ensemble des schémas fonctionnels construits à l'aide de $F^0_{\mathscr{L}} \cup V_{\mathscr{L}}$ comme ensemble de symboles à 0 variables, et de $F^n_{\mathscr{L}}$ comme ensemble de symboles à n variables $(n = 1, 2, ...)$. *Nous désignerons par* $T^n_{\mathscr{L}}$ *l'ensemble des termes où apparaissent* n *variables distinctes.*

On appelle ensemble des formules atomiques du langage $\mathscr{L}$ *et on désigne par* $At_{\mathscr{L}}$ l'ensemble $\bigcup_{n \in N} R^n_{\mathscr{L}} \times (T_{\mathscr{L}})^n$. Une formule atomique du langage $\mathscr{L}$ est donc une suite $Rt_1\, t_2 \ldots t_n$, où R est un symbole relationnel à n variables et où $t_1, t_2, \ldots, t_n$ sont des termes du langage $\mathscr{L}$. Pour faciliter la lecture, cette formule sera écrite aussi $R(t_1, \ldots, t_n)$, surtout lorsque l'un des termes t_i a une longueur > 1.

On appelle ensemble des formules du langage $\mathscr{L}$ *et on désigne par* $\mathscr{F}_{\mathscr{L}}$ *l'ensemble des schémas fonctionnels construits à l'aide des symboles suivants* :

α) Les symboles à 0 variables sont d'une part les formules atomiques, d'autre part $\top$ et $\bot$ (lire « vrai » et « faux »). L'ensemble des symboles à 0 variables est donc $At_{\mathscr{L}} \cup \{ \top \} \cup \{ \bot \}$.

β) Les symboles à 1 variable sont d'une part $\neg$ (lire « non ») d'autre part les éléments d'un ensemble Q disjoint des précédents et en correspondance biunivoque avec $V_{\mathscr{L}}$. L'élément de Q correspondant à la variable x sera noté $\vee x$ (lire « il existe un x »).

γ) Un seul symbole à 2 variables : $\vee$ (lire « ou »).

Remarque. — $\mathscr{F}_{\mathscr{L}} =$ Prop (P) au sens du chapitre précédent où P est le sous-ensemble de $\mathscr{F}_{\mathscr{L}}$ constitué par les éléments (formules) de $\mathscr{F}_{\mathscr{L}}$ dont le premier symbole n'est pas une constante propositionnelle ($\top$, $\bot$, $\neg$ ou $\vee$).

UNE RÉALISATION DU LANGAGE $\mathscr{L}$ est par définition constituée par :

1° *Un ensemble* $E \neq \phi$ appelé ensemble de base de la réalisation.

2° *Pour chaque* $n \geqslant 0$ *une application de* $F^n_{\mathscr{L}}$ *dans l'ensemble des fonctions*

définies sur E^n à valeurs dans E. On en déduit (théorème sur les schémas fonctionnels) une application de $T^n_{\mathscr{L}}$ dans l'ensemble des fonctions définies sur E^n à valeurs dans E.

3° *Pour chaque $n \geqslant 0$ une application de* $R^n_{\mathscr{L}}$ *dans* $\mathfrak{P}(E^n)$ (ensemble des parties de E^n). On en déduit une application de $At_{\mathscr{L}}$ dans $\mathfrak{P}(E^{V_{\mathscr{L}}})$: l'image de la formule atomique $Rt_1 \dots t_n$ par cette application étant l'ensemble $\{ \delta \in E^{V_{\mathscr{L}}} : (\delta t_1, \dots, \delta t_n) \in \overline{R} \}$, où $\overline{R} \subset E^n$ est l'image de R par l'application donnée, et où δt_i désigne la valeur prise par la fonction déduite du terme t_i quand les variables prennent les valeurs attribuées par δ. ($\delta \in E^{V_{\mathscr{L}}}$ est une application de $V_{\mathscr{L}}$ dans E.)

D'après le théorème sur les schémas fonctionnels, à chaque formule du langage $\mathscr{L}$ correspond par la réalisation un sous-ensemble de $E^{V_{\mathscr{L}}}$ si on définit $\top$, $\bot$, $\neg$, $\vee$, $\mathsf{V}x$ comme fonctions sur $\mathfrak{P}(E^{V_{\mathscr{L}}})$ de la façon suivante :

$\top$ est la constante $E^{V_{\mathscr{L}}}$.
$\bot$ est la constante ϕ.
$\neg$ est définie comme l'application $X \to \complement X$ de $\mathfrak{P}(E^{V_{\mathscr{L}}})$ dans lui-même.
$\vee$ est définie comme l'application $(X, Y) \to X \cup Y$ de $\{\mathfrak{P}(E^{V_{\mathscr{L}}})\}^2$ dans $\mathfrak{P}(E^{V_{\mathscr{L}}})$.
$\mathsf{V}x$ est définie comme l'application $X \to$ projection de X suivant la variable x (c'est-à-dire $\{ \delta \in E^{V_{\mathscr{L}}}$: il existe $\delta' \in X$ tel que $\delta' = \delta$ sauf peut-être sur $x \}$) de $\mathfrak{P}(E^{V_{\mathscr{L}}})$ dans lui-même.

(Dans l'exercice 1, nous donnons un exemple simple de langage et de réalisation de ce langage, permettant de suivre les constructions effectuées ici.)

Remarque. — Chaque fois que nous n'aurons à considérer qu'une seule réalisation à la fois du langage $\mathscr{L}$, nous noterons $\overline{A}$ la valeur prise par la formule A dans cette réalisation ($\overline{A} \subset E^{V_{\mathscr{L}}}$ si E est l'ensemble de base de la réalisation).

On dit qu'un sous-ensemble X de $E^{V_{\mathscr{L}}}$ ne *dépend* que des variables $x_1, \dots, x_n$ s'il existe $Y \subset E^{(x_1, \dots, x_n)}$ tel que $X = Y \times E^{V_{\mathscr{L}} - (x_1, \dots, x_n)}$.

Etant donnée une formule A, soient $x_1, \dots, x_n$ les variables apparaissant dans les termes de A. Alors dans toute réalisation, $\overline{A}$ ne dépend que de $x_1, \dots, x_n$.

Cet énoncé est évident si A est atomique. Si A et B satisfont à cet énoncé, $A \vee B$ et $\neg A$ y satisfont (car $\overline{A \vee B} = \overline{A} \cup \overline{B}$ et $\overline{\neg A} = \complement \overline{A}$ dans toute réalisation) ainsi que $\mathsf{V}xA$ (car $\overline{\mathsf{V}xA}$ = projection de $\overline{A}$ suivant la variable x). D'après la définition de l'ensemble des formules toute formule satisfait donc à cet énoncé.

Pour utiliser plus commodément ce genre de raisonnement appelons *longueur d'une formule A le nombre de constituants de A du type α, β, γ* (nombre de formules atomiques + nombre de symboles $\top$, $\bot$, $\neg$, $\vee$, $\mathsf{V}x$ apparaissant dans A).

A toute formule A du langage $\mathscr{L}$ on va associer par récurrence sur sa longueur un ensemble fini de variables appelées *variables libres* de A de la façon suivante : si A est de longueur 1 (formule atomique ou $\top$, ou $\bot$) les variables libres de A sont celles qui apparaissent dans les termes de A. Supposons alors défini l'ensemble des variables libres pour chaque formule de longueur $\leqslant n - 1$ et soit A une formule de longueur n. Si A commence par $\neg$ ou par $\vee$, A s'écrit $\neg B$ ou bien $\vee BC$ (B et C étant des formules). Alors les variables libres de A sont celles de B dans le 1[er] cas, celles de B et celles de C dans le 2[e]. Si A commence par $\mathsf{V}x$, A s'écrit $\mathsf{V}xB$. Alors les variables libres de A sont celles de B sauf x s'il y a lieu (c'est-à-dire si x est variable libre de B).

Une variable qui n'est pas libre dans A est dite *liée* dans A (en particulier toutes les variables qui n'apparaissent pas dans A sont liées dans A).

THÉORÈME. — *Soit A une formule dont les variables libres sont $x_1, ..., x_n$. Alors dans toute réalisation $\bar{A}$ ne dépend que des variables $x_1, ..., x_n$.*

Démonstration immédiate par récurrence sur la longueur de A.

Une formule A est dite close si elle n'a pas de variables libres. Il résulte du théorème précédent, que *dans une réalisation de base E, si A est close on a soit $\bar{A} = \phi$, soit $\bar{A} = E^{V_{\mathscr{L}}}$.*

On dit qu'une réalisation (de base E) satisfait une formule close si dans cette réalisation on a $\bar{A} = E^{V_{\mathscr{L}}}$. On dit encore que la réalisation est un modèle de A.

Etant donné un ensemble $\mathscr{A}$ de formules closes de $\mathscr{L}$, on dit qu'une réalisation de $\mathscr{L}$ satisfait $\mathscr{A}$ ou est un modèle de $\mathscr{A}$ si elle satisfait chaque formule de $\mathscr{A}$.

Notations. — A et B étant 2 formules de $\mathscr{L}$, $\vee AB$ sera aussi notée $(A) \vee (B)$; $(\neg A) \vee (B)$ sera notée $A \to B$; $\neg((\neg A) \vee (\neg B))$ sera notée $(A) \wedge (B)$; $\neg \mathsf{V}x \neg A$ sera notée ΛxA (le signe Λx se lisant « pour tout x »).

Une formule A dont les variables libres sont $x_1, ..., x_n$ sera notée $A(x_1, ..., x_n)$ lorsqu'on voudra mettre en évidence les variables libres ; on appelle clôture de A la formule $\Lambda x_1 \Lambda x_2 ... \Lambda x_n A$. La clôture de A est donc une formule close. Si $t_1, ..., t_n$ sont des termes, on notera $A(t_1, ..., t_n)$ la formule obtenue en remplaçant dans $A(x_1, ..., x_n)$ *chaque* occurrence de $x_1, ..., x_n$ respectivement par $t_1, ..., t_n$; c'est une formule d'après le chapitre 0.

Une formule A (non forcément close) est appelée théorème du langage $\mathscr{L}$ ou encore formule valide du langage $\mathscr{L}$ si dans toute réalisation on a $\bar{A} = E^{V_{\mathscr{L}}}$ (E étant l'ensemble de base de la réalisation). Cela revient à dire que toute réalisation satisfait la clôture de A.

Formules sans quantificateur : on appelle formule sans quantificateur du langage $\mathscr{L}$ une formule du calcul propositionnel construit sur $At_{\mathscr{L}}$ comme ensemble de variables propositionnelles. (Il est immédiat que c'est bien une

formule du langage $\mathscr{L}$. L'appellation vient du fait que $\mathsf{V}x$ et $\wedge x$ sont appelés quantificateurs.)

Formules prénexes : une formule est dite prénexe si elle s'écrit sous la forme QA, où Q est une suite finie de signes $\neg$ et $\mathsf{V}x_i(x_i \in V_{\mathscr{L}})$ et où A est une formule sans quantificateurs.

THÉORÈME. — *Si $V_{\mathscr{L}}$ est infini, pour toute formule A, il existe une formule A' prénexe équivalente à A (c'est-à-dire telle que $A' \leftrightarrow A$ soit un théorème ou encore telle que $\bar{A}' = \bar{A}$ dans toute réalisation de $\mathscr{L}$).*

LEMME. — *Si A et B sont deux formules prénexes, il existe une formule prénexe C équivalente à $\vee AB$.*

Démonstration par récurrence sur la longueur de $\vee AB$: le lemme est évident si A et B sont sans quantificateur. Si A par exemple contient des quantificateurs, soit $\mathsf{V}x$ le premier quantificateur apparaissant dans A. Il est donc précédé par des signes $\neg$ qu'on peut évidemment supposer en nombre $\leqslant 1$. Soit x' une variable qui n'apparaît ni dans A ni dans B. (Il en existe puisque $V_{\mathscr{L}}$ est infini.)

Si $A = \mathsf{V}xA'$, soit A'' la formule obtenue en remplaçant dans A' la variable x par x' partout où elle apparaît. Alors $A \vee B$ équivaut à $(\mathsf{V}x' A'') \vee B$, donc à $\mathsf{V}x'(A'' \vee B)$. Comme A'' et B sont prénexes, il suffit d'appliquer l'hypothèse de récurrence pour trouver une formule prénexe C' équivalente à $A'' \vee B$. La formule cherchée est $C = \mathsf{V}x' C'$.

Si $A = \neg \mathsf{V}xA'$ soit encore A'' la formule obtenue en remplaçant dans A' la variable x partout où elle apparaît par x'. Il est clair que A équivaut à $\neg \mathsf{V}x' A'' = \wedge x' \neg A''$ et que A'' est plus courte que A. D'après l'hypothèse de récurrence il existe une formule prénexe C' équivalente à $\neg A'' \vee B$. Posons $C = \neg \mathsf{V}x' \neg C'$; C équivaut donc à $\wedge x'(\neg A'' \vee B)$, donc à $(\wedge x' \neg A'') \vee B$ puisque x' n'apparaît pas dans B. Donc C équivaut à $\vee AB$. C. q. f. d.

Le théorème se démontre alors par récurrence sur la longueur de A : si A est atomique on pose $A' = A$. Si $A = \neg B$ ou $A = \mathsf{V}xB$, l'hypothèse de récurrence donne une formule B' prénexe équivalente à B. On pose alors $A' = \neg B'$ ou $A' = \mathsf{V}xB'$. Si $A = \vee BC$ l'hypothèse de récurrence donne deux formules prénexes B' et C' respectivement équivalentes à B et à C. Il suffit d'appliquer le lemme ci-dessus pour trouver une formule prénexe A' équivalente à $\vee B' C'$.
C. q. f. d.

Une formule prénexe peut toujours s'écrire sous la forme

$$Q_1 x_1 Q_2 x_2 \dots Q_n x_n H$$

où Q_i est un quantificateur ($Q_i = \wedge$ ou V) et où H est une formule sans quantificateurs. Elle sera dite purement existentielle si tous les Q_i sont V et purement universelle si tous les Q_i sont $\wedge$.

$\mathscr{E}$ étant un ensemble de formules de $\mathscr{L}$ *on appelle langage de* $\mathscr{E}$ *et on désigne par* $\mathscr{L}(\mathscr{E})$ le langage dont les variables sont celles de $\mathscr{L}$, et dont les symboles fonctionnels et relationnels sont ceux qui apparaissent dans les formules de $\mathscr{E}$.

On appelle réalisation canonique de $\mathscr{E}$ toute réalisation de $\mathscr{L}(\mathscr{E})$ dont l'ensemble de base est $T_{\mathscr{L}(\mathscr{E})}$ (ensemble des termes du langage de $\mathscr{E}$) et dans laquelle on donne aux symboles fonctionnels leur valeur canonique en tant que fonctions sur $T_{\mathscr{L}(\mathscr{E})}$ (on laisse donc libre le choix des valeurs des symboles relationnels).

Le but des théorèmes qui suivent (jusqu'au théorème d'uniformité) est de répondre à la question : étant donnée une formule A, que doit-on faire pour savoir si c'est un théorème ? (Voir aussi, appendice II, A, lemme 3). On se limite aux formules prénexes.

THÉORÈME. — *Soit* $\mathscr{E}$ *un ensemble de formules prénexes closes purement universelles. Si* $\mathscr{E}$ *a un modèle il a un modèle canonique.*

Nous posons $\mathscr{L}' = \mathscr{L}(\mathscr{E})$; toute formule de $\mathscr{E}$ est par hypothèse de la forme $\wedge x_1 \wedge x_2 \dots \wedge x_n A$, où A fait partie du calcul propositionnel construit sur les formules atomiques de $\mathscr{L}'$. Dans le modèle donné de $\mathscr{E}$, soit E l'ensemble de base et soit $\bar{R} \subset E^n$ la valeur attribuée au symbole relationnel $R \in R^n_{\mathscr{L}'}$. Soit δ un élément quelconque mais fixé de $E^{V_{\mathscr{L}'}}$. On en déduit une application $t \to \bar{t}$ de $T_{\mathscr{L}'}$ dans E. Nous définissons une réalisation canonique de $\mathscr{E}$ en donnant à $R \in R^n_{\mathscr{L}'}$ la valeur

$$\bar{\bar{R}} = \{ (t_1, \dots, t_n) \in (T_{\mathscr{L}'})^n : (\bar{t}_1, \bar{t}_2, \dots, \bar{t}_n) \in \bar{R} \} .$$

L'application $t \to \bar{t}$ de $T_{\mathscr{L}'}$ dans E définit une application $\varphi : (T_{\mathscr{L}'})^{V_{\mathscr{L}'}} \to E^{V_{\mathscr{L}'}}$ d'où l'application inverse $\varphi^{-1} : \mathfrak{P}(E^{V_{\mathscr{L}'}}) \to \mathfrak{P}((T_{\mathscr{L}'})^{V_{\mathscr{L}'}})$.

Si A est une formule sans quantificateurs de $\mathscr{L}'$, $\bar{A}$ étant la valeur qu'elle prend dans le modèle donné, $\bar{\bar{A}}$ celle qu'elle prend dans la réalisation canonique ci-dessus, on a $\bar{\bar{A}} = \varphi^{-1}(\bar{A})$: c'est clair si A est atomique, et on sait que φ^{-1} commute avec les opérations de réunion et de passage au complémentaire.

Soit alors $\wedge x_1 \dots \wedge x_n A$ une formule de $\mathscr{E}$. Par hypothèse on a $\bar{A} = E^{V_{\mathscr{L}'}}$. Donc

$$\bar{\bar{A}} = \varphi^{-1}(\bar{A}) = (T_{\mathscr{L}'})^{V_{\mathscr{L}'}} .$$

Donc $\wedge x_1 \dots \wedge x_n A$ est satisfaite dans la réalisation canonique considérée.

C. q. f. d.

THÉORÈME DUAL. — *Soit* A *une formule prénexe close purement existentielle. Pour que* A *soit un théorème, il faut et il suffit que toute réalisation canonique de* A *la satisfasse.*

La condition est évidemment nécessaire. Elle est suffisante, car si toute réalisation canonique satisfait A, aucune ne satisfait $\neg A$ qui n'a donc pas de modèle d'après le théorème précédent.

THÉORÈME. — *Pour toute formule prénexe F il existe une formule prénexe $\widehat{F}$ purement universelle, dont le langage ne diffère de celui de F que par l'adjonction d'un nombre fini de symboles fonctionnels, telle que :*

a) *Dans toute réalisation de $\mathscr{L}(\widehat{F})$ on a $\overline{\widehat{F}} \subset \overline{F}$ (c'est-à-dire $\widehat{F} \to F$ est un théorème).*

b) *Toute réalisation de $\mathscr{L}(F)$ se prolonge à $\mathscr{L}(\widehat{F})$ de façon que $\overline{F} = \overline{\widehat{F}}$.*

Par récurrence sur le nombre de quantificateurs de F. Si F n'en a aucun, on prend $\widehat{F} = F$.

Si $F = \bigwedge xG$, par hypothèse il y a une formule G satisfaisant au théorème pour G. Il suffit de poser $\widehat{F} = \bigwedge x\widehat{G}$.

Si $F = \bigvee xG$, soit $\widehat{G}$ une formule satisfaisant au théorème pour G. Soient $x_0, x_1, ..., x_n$ les variables libres de $\widehat{G}$. Si x n'est pas libre dans $\widehat{G}$, dans toute réalisation on a $\overline{\bigvee x\widehat{G}} = \overline{\widehat{G}}$. Il suffit donc de prendre $\widehat{F} = \widehat{G}$.

Si x est libre dans $\widehat{G}$ on a par exemple $x_0 = x$. Soit alors φ un symbole fonctionnel à n variables qui ne soit pas dans $\mathscr{L}(\widehat{G})$. Soit $\widehat{F}$ la formule obtenue en remplaçant dans $\widehat{G}$, x par $\varphi x_1 \ldots x_n$. Il est clair que $\widehat{F}$ est purement universelle (puisque $\widehat{G}$ l'est). $\widehat{F}$ satisfait à la condition a) : soit E l'ensemble de base d'une réalisation de $\mathscr{L}(\widehat{F})$: $\overline{\widehat{F}}$ est l'ensemble des $(a_1, ..., a_n) \in E^{(x_1,...,x_n)}$ tels que

$$(\overline{\varphi}(a_1, ..., a_n), a_1, ..., a_n) \in \overline{\widehat{G}} \subset \overline{G} \subset E^{(x,x_1,...,x_n)}.$$

Donc pour tout élément $(a_1, ..., a_n)$ de $\overline{\widehat{F}}$, on a $(a_1, ..., a_n) \in \overline{\bigvee xG} = \overline{F}$. Donc $\overline{\widehat{F}} \subset \overline{F}$.

$\widehat{F}$ satisfait la condition b) : soit en effet E l'ensemble de base d'une réalisation de $\mathscr{L}(F)$. Par hypothèse on peut prolonger cette réalisation à $\mathscr{L}(\widehat{G})$ de façon que $\overline{G} = \overline{\widehat{G}}$. On a alors $\overline{F} = \overline{\bigvee xG} = \overline{\bigvee x\widehat{G}}$. Donc pour que

$$(a_1, ..., a_n) \in E^{(x_1,...,x_n)}$$

soit dans $\overline{F}$, il faut et il suffit qu'il existe un $a \in E$ tel que $(a, a_1, ..., a_n) \in \overline{\widehat{G}}$. On définit alors $\overline{\varphi}$ (on a encore le choix de sa définition puisque $\varphi \notin \mathscr{L}(\widehat{G})$ par hypothèse) de la façon suivante :

$$\overline{\varphi}(a_1, ..., a_n) = a \qquad \text{si} \qquad (a_1, ..., a_n) \in \overline{F}$$

$$\overline{\varphi}(a_1, ..., a_n) = a_0 \quad \text{(élément quelconque de } E\text{)} \quad \text{si } (a_1, ..., a_n) \notin \overline{F}.$$

On obtient ainsi une réalisation de $\mathscr{L}(\widehat{F})$; dans cette réalisation $\overline{\widehat{F}}$ est l'ensemble des $(a_1, ..., a_n)$ tels que $(\overline{\varphi}(a_1, ..., a_n), a_1, ..., a_n) \in \overline{\widehat{G}}$. On a donc bien $\overline{\widehat{F}} = \overline{\bigvee x\widehat{G}} = \overline{F}$. C. q. f. d.

Théorème dual. — *Pour toute formule prénexe F, il existe une formule prénexe $\check{F}$, purement existentielle, dont le langage ne diffère de celui de F que par l'adjonction d'un nombre fini de symboles fonctionnels telle que :*

a) *Dans toute réalisation de $\mathscr{L}(\check{F})$ on a $\overline{\check{F}} \supset \overline{F}$ (c'est-à-dire $F \to \check{F}$ est un théorème).*

b) *Toute réalisation de $\mathscr{L}(F)$ se prolonge à $\mathscr{L}(\check{F})$ de façon que $\overline{F} = \overline{\check{F}}$.*

Il suffit de poser $\check{F} = \neg\, \widehat{(\neg F)}$.

Corollaire 1. — *Pour qu'une formule prénexe close F soit un théorème il faut et il suffit que $\check{F}$ soit satisfaite par toutes ses réalisations canoniques.*

Si F est un théorème, comme $F \to \check{F}$ en est un, $\check{F}$ en est un aussi, et par suite $\check{F}$ est satisfaite en particulier par toutes ses réalisations canoniques.

Inversement, si $\check{F}$ est satisfaite par toutes ses réalisations canoniques, comme elle est purement existentielle, c'est un théorème. Etant donnée une réalisation quelconque de $\mathscr{L}(F)$ on peut la prolonger de façon que $\overline{F} = \overline{\check{F}}$. Or $\check{F}$ est satisfaite par ce prolongement. Donc F est satisfaite par la réalisation donnée. F est donc un théorème.

Corollaire 2. — *Soit $\mathscr{E}$ un ensemble dénombrable de formules closes. S'il a un modèle il a un modèle dénombrable.*

On peut supposer $\mathscr{E}$ constitué par des formules prénexes. Soit alors $\widehat{\mathscr{E}}$ l'ensemble des $\hat{F}$ pour $F \in \mathscr{E}$ (les symboles fonctionnels ajoutés à $\mathscr{L}(\mathscr{E})$ pour chaque F étant supposés tous distincts).

$\mathscr{E}$ ayant un modèle celui-ci se prolonge en un modèle de $\widehat{\mathscr{E}}$. Or $\widehat{\mathscr{E}}$ est formé de formules prénexes purement universelles ; ayant un modèle il a donc un modèle canonique. Or ce dernier est évidemment dénombrable.

C. q. f. d.

On donne en exercice (nos 4-5) des énoncés plus précis de ce théorème.

Considérons un langage $\mathscr{L}$. Se donner une réalisation canonique de $\mathscr{L}$ revient à se donner pour chaque $n \geqslant 0$ une application de $R^n_{\mathscr{L}}$ dans

$$\mathfrak{P}[(T_{\mathscr{L}})^n] = \{0, 1\}^{(T_{\mathscr{L}})^n}.$$

Cela revient donc à se donner une application de $R^n_{\mathscr{L}} \times (T_{\mathscr{L}})^n$ dans $\{0, 1\}$, et ceci pour chaque $n \geqslant 0$, donc à se donner une application de $At_{\mathscr{L}}$ (ensemble des formules atomiques de $\mathscr{L}$) dans $\{0, 1\}$. Par suite :

La donnée d'une réalisation canonique d'un langage $\mathscr{L}$ est équivalente à la donnée d'une réalisation du calcul propositionnel construit sur les formules atomiques de $\mathscr{L}$.

LEMME. — *Soit $F(x_1, ..., x_m)$ une formule sans quantificateurs de $\mathcal{L}$, (dont les variables libres sont $x_1, ..., x_m$) et soient $t_1, ..., t_m$ des termes de $\mathcal{L}$. Pour que dans une réalisation canonique de $\mathcal{L}$ on ait $(t_1, ..., t_m) \in \overline{F}$, il faut et il suffit que la réalisation correspondante du calcul propositionnel construit sur $At_{\mathcal{L}}$ satisfasse $F(t_1, ..., t_m)$.*

Le lemme est évident si F est atomique. Il est clair que si F satisfait au lemme, $\neg F$ y satisfait aussi. De même si F, G satisfont au lemme $\vee FG$ y satisfait aussi : pour que $(t_1, ..., t_m) \in \overline{\vee FG}$, il faut et il suffit que $(t_1, ..., t_m) \in \overline{F}$ ou que $(t_1, ..., t_m) \in \overline{G}$, donc que $F(t_1, ..., t_m)$ ou $G(t_1, ..., t_m)$ soit satisfaite par la réalisation du calcul propositionnel construit sur $At_{\mathcal{L}}$, c'est-à-dire que $F(t_1, ..., t_m) \vee G(t_1, ..., t_m)$ soit satisfaite par cette réalisation.

THÉORÈME D'UNIFORMITÉ. — *Soit $F(x_1, ..., x_m)$ une formule sans quantificateurs dont les variables libres sont $x_1, ..., x_m$. Pour que*

$$\bigvee x_1 \bigvee x_2 ... \bigvee x_m \; F(x_1, ..., x_m)$$

soit un théorème, il faut et il suffit qu'il existe des termes $t_1^i, ..., t_m^i (1 \leqslant i \leqslant k)$ du langage de F, tels que la formule :

$$F(t_1^1, ..., t_m^1) \vee F(t_1^2, ..., t_m^2) \vee \cdots \vee F(t_1^k, ..., t_m^k)$$

soit un théorème du calcul propositionnel construit sur les formules atomiques de $\mathcal{L}(F)$.

La condition est suffisante : supposons en effet que la formule

$$F(t_1^1, ..., t_m^1) \vee \cdots \vee F(t_1^k, ..., t_m^k)$$

soit un théorème du calcul propositionnel construit sur $At_{\mathcal{L}(F)}$. Considérons une réalisation canonique quelconque de $\mathcal{L}(F)$. Dans la réalisation correspondante du calcul propositionnel construit sur $At_{\mathcal{L}(F)}$ la formule précédente est satisfaite, donc par exemple $F(t_1^1, ..., t_m^1)$ est satisfaite. Le lemme montre alors que dans la réalisation canonique considérée on a $(t_1^1, ..., t_m^1) \in \overline{F}$. Par suite $\bigvee x_1 ... \bigvee x_m \; F(x_1, ..., x_m)$ est satisfaite. Cette formule purement existentielle étant satisfaite par toutes ses réalisations canoniques est un théorème.

La condition est nécessaire : si $\bigvee x_1 ... \bigvee x_m \; F(x_1, ..., x_m)$ est un théorème, elle est satisfaite par toutes ses réalisations canoniques. Donc pour toute réalisation canonique de $\mathcal{L}(F)$, il existe des termes $t_1, ..., t_m$ de $\mathcal{L}(F)$ tels que $(t_1, ..., t_m) \in \overline{F}$. D'après le lemme il en résulte que pour toute réalisation du calcul propositionnel construit sur $At_{\mathcal{L}(F)}$, il existe des termes $t_1, ..., t_m$ tels que $F(t_1, ..., t_m)$ soit satisfaite. Le deuxième énoncé (p. 8) du théorème de finitude du calcul propositionnel montre qu'il existe des termes $t_1^i, ..., t_m^i (1 \leqslant i \leqslant k)$ tels que

$$F(t_1^1, ..., t_m^1) \vee \cdots \vee F(t_1^k, ..., t_m^k)$$

soit un théorème du calcul propositionnel construit sur $At_{\mathcal{L}(F)}$. C. q. f. d.

D'après ce qui précède on a donc la méthode suivante pour vérifier qu'une formule A prénexe est un théorème : on forme $\check{A}$ qui, étant purement existentielle, se met sous la forme $\bigvee x_1 \ldots \bigvee x_m\, F(x_1, \ldots, x_m)$, où F est sans quantificateurs. Il suffit alors d'essayer toutes les formules de la forme

$$F(t_1^1, \ldots, t_m^1) \vee \cdots \vee F(t_1^k, \ldots, t_m^k) ,$$

où les t_i sont des termes de $\mathscr{L}(F)$, jusqu'à ce qu'on tombe sur un théorème du calcul propositionnel construit sur $At_{\mathscr{L}(F)}$ (ce qu'il est facile de vérifier pour chaque formule considérée en un nombre fini d'essais, d'après la définition même d'un théorème du calcul propositionnel). A est un théorème si et seulement si cet événement se produit.

THÉORÈME DE FINITUDE. — *Pour qu'un ensemble $\mathscr{E}$ de formules closes ait un modèle, il faut et il suffit que tout sous-ensemble fini de $\mathscr{E}$ en ait un.*

Désignons par $\mathscr{L}$ le langage de $\mathscr{E}$. On peut évidemment supposer $\mathscr{E}$ constitué de formules prénexes. Soit alors $\hat{\mathscr{E}}$ l'ensemble des $\hat{A}$ quand A décrit $\mathscr{E}$ (les symboles fonctionnels ajoutés à $\mathscr{L}$ pour chaque A étant supposés tous distincts et non dans $\mathscr{L}$). Comme $\hat{A} \rightarrow A$ est un théorème il suffit de montrer que $\hat{\mathscr{E}}$ a un modèle.

Tout sous-ensemble fini de $\hat{\mathscr{E}}$ a un modèle : en effet si $\{ \hat{A}_1, \ldots, \hat{A}_n \}$ est un sous-ensemble fini de $\mathscr{E}$, par hypothèse $\{ A_1, \ldots, A_n \}$ a un modèle et on sait qu'on peut le prolonger en un modèle de $\{ \hat{A}_1, \ldots, \hat{A}_n \}$ (théorème, page 19). On est donc ramené à démontrer le théorème dans le cas où l'ensemble $\mathscr{E}$ est formé de formules prénexes purement universelles.

Ecrivons chaque formule A de $\mathscr{E}$ sous la forme $A = \bigwedge x_1 \ldots \bigwedge x_m\, A_0(x_1, \ldots, x_m)$ où A_0 est sans quantificateurs et soit $\mathscr{A}$ l'ensemble des formules $A_0(t_1, \ldots, t_m)$ du calcul propositionnel construit sur $At_{\mathscr{L}}$, quand A décrit $\mathscr{E}$ et que les t_i décrivent $T_{\mathscr{L}}$.

Tout sous-ensemble fini de $\mathscr{E}$, ayant un modèle, a un modèle canonique. Il en résulte (lemme p. 21) que tout sous-ensemble fini de $\mathscr{A}$ a un modèle (au sens du calcul propositionnel). Donc que $\mathscr{A}$ tout entier a un modèle (théorème de finitude pour le calcul propositionnel). C'est une conséquence immédiate du lemme p. 21 que la réalisation canonique correspondant à ce modèle satisfait $\mathscr{E}$. C. q. f. d.

Notations. — Dans la suite on utilisera les notations suivantes :

1° $\mathscr{L}$ et $\mathscr{L}'$ étant deux langages, $\mathscr{L} \cup \mathscr{L}'$ désignera le langage dont les symboles fonctionnels et relationnels sont ceux de $\mathscr{L}$ et de $\mathscr{L}'$, $\mathscr{L} \cap \mathscr{L}'$ désignera le langage dont les symboles fonctionnels et relationnels sont ceux communs à $\mathscr{L}$ et $\mathscr{L}'$; $\mathscr{L} \subset \mathscr{L}'$ signifiera que tous les symboles fonctionnels et relationnels qui sont dans $\mathscr{L}$ sont aussi dans $\mathscr{L}'$. On a par exemple $\mathscr{L}(\vee AB) = \mathscr{L}(A) \cup \mathscr{L}(B)$.

2° $A_1, \ldots, A_n$ étant des formules, la formule $A_1 \vee \cdots \vee A_n$ sera écrite $\bigvee_{i=1}^{n} A_i$, la formule $A_1 \wedge \cdots \wedge A_n$ sera écrite $\bigwedge_{i=1}^{n} A_i$.

LEMME D'INTERPOLATION. — *Si $A \vee B$ est un théorème, il existe une formule C telle que $\mathscr{L}(C) \subset \mathscr{L}(A) \cap \mathscr{L}(B)$ et telle que $A \vee C$ et $B \vee \neg C$ soient des théorèmes.*

On peut supposer A et B closes : en effet supposons le théorème démontré dans ce cas et soient $A(z_1, ..., z_k)$ et $B(z_1, ..., z_k)$ deux formules dont les variables libres sont parmi $z_1, ..., z_k$ et telles que $A(z_1, ..., z_k) \vee B(z_1, ..., z_k)$ soit un théorème. Soient $a_1, ..., a_k$, k symboles de constantes (symboles fonctionnels à 0 variable) non dans $\mathscr{L}(A) \cup \mathscr{L}(B)$. Alors $A(a_1, ..., a_k) \vee B(a_1, ..., a_k)$ est un théorème. Par hypothèse il existe une formule D telle que

$$\mathscr{L}(D) \subset \{ \mathscr{L}(A) \cap \mathscr{L}(B) \} \cup (a_1, ..., a_k)$$

et telle que $A(a_1, ..., a_k) \vee D$ et $B(a_1, ..., a_k) \vee \neg D$ soient des théorèmes. En désignant par C la formule obtenue en substituant $z_1, ..., z_k$ à $a_1, ..., a_k$ dans D, on voit immédiatement que C satisfait au théorème pour $A(z_1, ..., z_k)$ et $B(z_1, ..., z_k)$.

A et B étant maintenant supposées closes, on peut les supposer purement existentielles. Supposons en effet le théorème démontré dans ce cas, et soient A, B deux formules prénexes telles que $A \vee B$ soit un théorème. Formons $\check{A}$ et $\check{B}$ avec des symboles fonctionnels distincts et non dans $\mathscr{L}(A) \cup \mathscr{L}(B)$ (de façon que $\mathscr{L}(\check{A}) \cap \mathscr{L}(\check{B}) = \mathscr{L}(A) \cap \mathscr{L}(B)$). Comme $A \to \check{A}$ et $B \to \check{B}$ sont des théorèmes ainsi que $A \vee B$, $\check{A} \vee \check{B}$ en est un aussi. D'où l'existence d'une formule C, telle que $\mathscr{L}(C) \subset \mathscr{L}(A) \cap \mathscr{L}(B)$ et telle que $\check{A} \vee C$ et $\check{B} \vee \neg C$ soient des théorèmes. Or toute réalisation de $\mathscr{L}(A)$ donc de $\mathscr{L}(A \vee C)$ se prolonge à $\mathscr{L}(\check{A})$ de façon que $\overline{A} = \overline{\check{A}}$, donc de façon que

$$\overline{A \vee C} = \overline{\check{A} \vee C}\,.$$

Il en résulte que toute réalisation de $\mathscr{L}(A)$ satisfait $A \vee C$ qui est donc un théorème. De même $B \vee \neg C$ est un théorème.

On peut donc supposer maintenant que $A = \bigvee x_1 ... \bigvee x_m\, H(x_1, ..., x_m)$ et que $B = \bigvee y_1 ... \bigvee y_m\, K(y_1, ..., y_m)$, H et K étant sans quantificateurs. Comme $A \vee B$ est un théorème, d'après le théorème d'uniformité il existe des termes t_i^h et u_j^k de $\mathscr{L}(A \vee B)$ tels que si

$$A_1 = \bigvee_h H(t_1^h, ..., t_m^h) \qquad \text{et} \qquad B_1 = \bigvee_k K(u_1^k, ..., u_n^k)\,,$$

$A_1 \vee B_1$ soit un théorème du calcul propositionnel construit sur les formules atomiques de $\mathscr{L}(A \vee B)$. D'après le lemme d'interpolation du calcul propositionnel, il existe une formule C dont les variables propositionnelles sont communes à A_1 et B_1 et telle que $A_1 \vee C$ et $B_1 \vee \neg C$ soient deux théorèmes du calcul propositionnel.

Soient $\xi_1, ..., \xi_l$ les termes apparaissant dans les formules atomiques de C. On a donc $C = C_1(\xi_1, ..., \xi_l)$ où $C_1(z_1, ..., z_l)$ est une formule dont les variables

libres sont $z_1, ..., z_l$, sans symboles fonctionnels et dont les symboles relationnels sont dans $\mathscr{L}(A) \cap \mathscr{L}(B)$.

Construisons par récurrence sur p une suite de formules sans quantificateurs $C_p(z_1, ..., z_{l_p})$, dont le langage soit contenu dans $\mathscr{L}(A) \cap \mathscr{L}(B)$, et pour chaque p une suite $\xi_1^p, ..., \xi_{l_p}^p$ de termes de $\mathscr{L}(A) \cup \mathscr{L}(B)$ de la façon suivante :

Pour $p = 1$ la formule est $C_1(z_1, ..., z_l)$ et la suite de termes $\xi_1, ..., \xi_l$. Supposons la construction faite jusqu'au rang p de façon que l'on ait $C = C_p(\xi_1^p, ..., \xi_{l_p}^p)$. Choisissons un ξ_i^p de longueur maximum qui commence par un symbole fonctionnel $\varphi \in \mathscr{L}(A) \cap \mathscr{L}(B)$ (s'il existe un tel ξ_i^p). On a alors, si par exemple $\xi_{l_p}^p$ est ce terme : $\xi_{l_p}^p = \varphi\eta_1 ... \eta_r$ où $\eta_1, ..., \eta_r$ sont des termes de $\mathscr{L}(A) \cup \mathscr{L}(B)$. On pose alors

$$C_{p+1}(z_1, ..., z_{l_{p+1}}) = C_p(z_1, ..., z_{l_p - 1}, \varphi z_{l_p} ... z_{l_p + r})$$

et on définit la suite de termes au rang $p + 1$ comme étant $\xi_1, ..., \xi_{l_p - 1}, \eta_1, ..., \eta_r$.

Il est immédiat que quand p augmente d'une unité la somme des longueurs des termes de la suite diminue d'une unité. Il en résulte que la construction devient impossible au bout d'un nombre fini de pas. On a alors une formule $M(z_1, ..., z_q)$ et une suite de termes $\eta_1, ..., \eta_q$ tels que : $C = M(\eta_1, ..., \eta_q)$; le langage de $M(z_1, ..., z_q)$ est contenu dans $\mathscr{L}(A) \cap \mathscr{L}(B)$; aucun des termes $\eta_1, ..., \eta_q$ ne commence par un symbole fonctionnel de $\mathscr{L}(A) \cap \mathscr{L}(B)$.

Puisque $A_1 \vee C$ et $B_1 \vee \neg C$ sont des théorèmes du calcul propositionnel construit sur les formules atomiques de $\mathscr{L}(A) \cup \mathscr{L}(B)$, le lemme (p. 21) montre que

$$\bigvee x_1 ... \bigvee x_m\, H(x_1, ..., x_m) \vee M(\eta_1, ..., \eta_q)$$

et

$$\bigvee y_1 ... \bigvee y_n\, K(y_1, ..., y_n) \vee \neg M(\eta_1, ..., \eta_q)$$

sont deux théorèmes. Supposons $\eta_1, ..., \eta_q$ rangés par ordre de longueur non croissant (de façon qu'aucun d'eux ne puisse être un sous-terme de l'un des suivants).

Posons

$$C = Q_q z_q\, Q_{q-1} z_{q-1} ... Q_1 z_1\, M(z_1, ..., z_q)\,,$$

où $Q_i = \bigwedge$ si η_i commence par un symbole φ de $\mathscr{L}(B)$ (donc $\varphi \notin \mathscr{L}(A)$) et $Q_i = \bigvee$ si η_i commence par un symbole φ de $\mathscr{L}(A)$ (donc $\varphi \notin \mathscr{L}(B)$). On va voir que C est la formule cherchée.

Il est d'abord immédiat que

$$\mathscr{L}(C) \subset \mathscr{L}(A) \cap \mathscr{L}(B) \quad (\text{car} \quad \mathscr{L}(M) \subset \mathscr{L}(A) \cap \mathscr{L}(B)).$$

Supposons alors montré pour $l \leqslant q$ que :

$$A \vee Q_{l-1}\, z_{l-1} \ldots Q_1\, z_1\, M(z_1, \ldots, z_{l-1}, \eta_l, \ldots, \eta_q)$$

et

$$B \vee \neg\, Q_{l-1}\, z_{l-1} \ldots Q_1\, z_1\, M(z_1, \ldots, z_{l-1}, \eta_l, \ldots, \eta_q)$$

sont deux théorèmes. (Ce qui est vrai pour $l = 1$.)

Posons

$$U(z_l) = Q_{l-1}\, z_{l-1} \ldots Q_1\, z_1\, M(z_1, \ldots, z_{l-1}, z_l, \eta_{l+1}, \ldots, \eta_q) \;.$$

Par hypothèse on a donc les deux théorèmes : $A \vee U(\eta_l)$; $B \vee \neg\, U(\eta_l)$. Supposons par exemple que η_l commence par un symbole $\varphi \in \mathscr{L}(B)$ et donc $\notin \mathscr{L}(A)$, et posons $\eta_l = \varphi\tau_1, \ldots, \tau_r$, $\tau_1 \ldots \tau_r$ étant des termes de $\mathscr{L}(A) \cup \mathscr{L}(B)$. On a à montrer que $A \vee \bigwedge z_l\, U(z_l)$ et $B \vee \bigvee z_l \neg\, U(z_l)$ sont deux théorèmes. C'est évident pour le second puisque $B \vee \neg\, U(\eta_l)$ est un théorème.

On pose $A \vee U(z_l) = V(z_l, \eta_{l+1}, \ldots, \eta_q)$, avec

$$V(z_l, z_{l+1}, \ldots, z_q) = A \vee Q_{l-1}\, z_{l-1} \ldots Q_1\, z_1\, M(z_1, \ldots, z_{l-1}, z_l, \ldots, z_q) \,.$$

On a à montrer que $\bigwedge z_l\, V(z_l, \eta_{l+1}, \ldots, \eta_q)$ est un théorème. C'est une conséquence du lemme suivant :

LEMME. — *Soit $V(z, \eta_1, \ldots, \eta_q)$ une formule à une variable libre z, et soit φ un symbole fonctionnel qui n'est pas dans $V(z, z_1, \ldots, z_q)$. Soit $\eta = \varphi\tau_1 \ldots \tau_r$ un terme commençant par φ, au moins aussi long que $\eta_1, \ldots, \eta_q$, différent de $\eta_1, \ldots, \eta_q$, et tel que $V(\eta, \eta_1, \ldots, \eta_q)$ soit un théorème. Alors $\bigwedge z V(z, \eta_1, \ldots, \eta_q)$ est un théorème.*

On peut se ramener au cas où V est purement existentielle, en la remplaçant au besoin par $\check{V}$: si $V(\eta, \eta_1, \ldots, \eta_q)$ est un théorème, $\check{V}(\eta, \eta_1, \ldots, \eta_q)$ en est un ; donc (en appliquant le lemme à cette formule existentielle) $\bigwedge z \check{V}(z, \eta_1, \ldots, \eta_q)$ en est un. Si a est un nouveau symbole de constante, $\check{V}(a, \eta_1, \ldots, \eta_q)$ qui est aussi $[\bigwedge z V(z, \eta_1, \ldots, \eta_q)]^{\vee}$, est un théorème, et donc aussi $\bigwedge z V(z, \eta_1, \ldots, \eta_q)$.

On peut donc prendre

$$V(z, \eta_1, \ldots, \eta_q) = \bigvee x_1 \ldots \bigvee x_m\, W(z, \eta_1, \ldots, \eta_q, x_1, \ldots, x_m) \,.$$

Soit a un nouveau symbole de constante ; on a à montrer que $V(a, \eta_1, \ldots, \eta_q)$ est un théorème ; donc qu'elle est satisfaite par chaque réalisation canonique $\mathfrak{M}$. Soit $\mathfrak{M}'$ la réalisation obtenue à partir de $\mathfrak{M}$, en changeant la valeur de φ au point $(\tau_1, \ldots, \tau_r)$, en posant $\varphi(\tau_1, \ldots, \tau_r) = a$ au lieu de $\varphi(\tau_1, \ldots, \tau_r) = \varphi\tau_1 \ldots \tau_r$ ce qui avait lieu dans la réalisation canonique $\mathfrak{M}$. La réalisation $\mathfrak{M}'$ satisfait $V(\eta, \eta_1, \ldots, \eta_q)$ qui est un théorème. Les valeurs prises par $\eta_1, \ldots, \eta_q$ sont les mêmes dans $\mathfrak{M}$ et dans $\mathfrak{M}'$ (et sont $\eta_1, \ldots, \eta_q$ eux-mêmes) puisque aucun d'eux ne contient η. Les valeurs prises par la formule $W(z, z_1, \ldots, z_q, x_1, \ldots, x_m)$ dans

$\mathfrak{M}$ et dans $\mathfrak{M}'$ sont les mêmes puisque cette formule ne contient pas φ ; soit $\overline{W}$ cette valeur. Puisque $\mathfrak{M}'$ satisfait

$$\vee x_1 \dots \vee x_m\, W(\eta, \eta_1, \dots, \eta_q, x_1, \dots, x_m)$$

il existe des termes $t_1, \dots, t_m$ tels que

$$(\bar{\eta}, \bar{\eta}_1, \dots, \bar{\eta}_q, t_1, \dots, t_m) \in \overline{W}$$

en effet $\mathfrak{M}'$ a pour ensemble de base l'ensemble des termes. Or $\bar{\eta}_1 = \eta_1, \dots, \bar{\eta}_q = \eta_q$, et $\bar{\eta} = a$; donc

$$(a, \eta_1, \dots, \eta_q, t_1, \dots, t_m) \in \overline{W},$$

ce qui veut dire que $W(a, \eta_1, \dots, \eta_q, t_1, \dots, t_m)$ est satisfaite dans $\mathfrak{M}$, donc aussi $V(a, \eta_1, \dots, \eta_q)$. C. q. f. d.

Dans l'exercice 7 nous donnons un exemple où la formule C est obtenue en suivant la démonstration ci-dessus.

Autre énoncé. — *Si $A \to B$ est un théorème, il existe une formule C telle que $\mathscr{L}(C) \subset \mathscr{L}(A) \cap \mathscr{L}(B)$ et telle que $A \to C$ et $C \to B$ soient des théorèmes.*

Corollaire : théorème de définissabilité.

Soit $\mathscr{A}$ un ensemble de formules, R un symbole relationnel à n variables de $\mathscr{L}(\mathscr{A})$, $\mathscr{A}'$ l'ensemble des formules obtenues en substituant à R dans chaque formule de $\mathscr{A}$ un symbole relationnel R' à n variables non dans $\mathscr{L}(\mathscr{A})$. Alors si

$$Rx_1 \dots x_n \to R'\, x_1 \dots x_n$$

est conséquence de $\mathscr{A} \cup \mathscr{A}'$, il existe une formule F telle que $\mathscr{L}(F) \subset \mathscr{L}(\mathscr{A})$ et $R \notin \mathscr{L}(F)$ et telle que $(F \leftrightarrow Rx_1, \dots, x_n)$ soit conséquence de $\mathscr{A}$.

En effet puisque $(Rx_1 \dots x_n \to R'\, x_1 \dots x_n)$ est conséquence de $\mathscr{A} \cup \mathscr{A}'$ il y a un sous-ensemble fini $\mathscr{A}_1 \subset \mathscr{A}$ tel que $(Rx_1 \dots x_n \to R'\, x_1 \dots x_n)$ soit conséquence de $\mathscr{A}_1 \cup \mathscr{A}'_1$ (théorème de finitude). Si A est la conjonction des formules de $\mathscr{A}_1$,

$$A \wedge A' \to (Rx_1 \dots x_n \to R'\, x_1 \dots x_n)$$

est un théorème et, par conséquent,

$$A \wedge Rx_1 \dots x_n \to (A' \to R'\, x_1 \dots x_n)$$

en est un aussi. D'après le lemme d'interpolation, il y a une formule F telle que $\mathscr{L}(F) \subset \mathscr{L}(A) \cap \mathscr{L}(A')$ et telle que

$$A \wedge Rx_1 \dots x_n \to F \quad \text{et} \quad F \to (A' \to R'\, x_1 \dots x_n)$$

soient des théorèmes. Donc

$$A \to (Rx_1 \dots x_n \to F) \text{ et } A' \to (F \to R'x_1 \dots x_n)$$

sont des théorèmes.

C. q. f. d.

EXERCICES

1. On donne le langage $\mathscr{L}$ suivant :

$V_{\mathscr{L}}$ est l'ensemble $\{x, y\}$ (deux éléments).
$F_{\mathscr{L}}$ est constitué par un seul symbole f à une seule variable.
$R_{\mathscr{L}}$ a deux éléments : U à une variable, R à 2 variables.

On considère la réalisation suivante de $\mathscr{L}$: l'ensemble de base est $\mathbf{R}$ (ensemble des réels). La valeur prise par U est le segment [0, 1]. La valeur prise par R est $\overline{R} = \{(x, y) \in \mathbf{R}^2 : x < y\}$. La valeur prise par f est $x \to x^2 + 1$.

Quel est l'ensemble des termes de $\mathscr{L}$?

Les valeurs prises par les formules de $\mathscr{L}$ peuvent être représentées comme sous-ensemble du plan $\mathbf{R}^{\{x,y\}}$. Quels sont les sous-ensembles du plan correspondant aux formules Ux ; Ufx ; $\bigvee xUfx$; Rx, fy ; $\bigwedge xRy, fx$; $\bigwedge xRx, fy$; $\bigwedge xRx, fx$; $\bigwedge y(Uy \to Rfy, x)$.

2. Donner une formule prénexe équivalente à

$$\bigwedge x \bigvee y \bigwedge zAxyz \to \bigwedge y \bigvee zByz \qquad (A \in R^3_{\mathscr{L}} \,;\, B \in R^2_{\mathscr{L}})\,.$$

3. On considère la formule F : $\bigwedge x \bigvee y \bigvee z \bigwedge u \bigvee vAx\,y\,z\,u\,v$, où A est un symbole relationnel à 5 variables. Donner deux formules $\widehat{F}$ et $\check{F}$ satisfaisant aux théorèmes p. 19 et p. 20.

Solution. — La méthode de démonstration des théorèmes considérés donne les deux formules $\widehat{F} = \bigwedge x \bigwedge uA(x, fx, gx, u, hxfxgxu)$ (où f, g sont des symboles fonctionnels à 1 variable et h un symbole fonctionnel à 4 variables)

$$\check{F} = \bigvee y \bigvee z \bigvee vA(a, y, z, \varphi ayz, v)$$

(où a est un symbole fonctionnel à 0 variable et φ un symbole fonctionnel à 3 variables).

4. Soit $\mathscr{E}$ un ensemble de formules de cardinal $\aleph \geqslant \aleph_0$. Montrer que si $\mathscr{E}$ a un modèle, pour tout cardinal $\aleph' \geqslant \aleph$ il a un modèle de cardinal $\aleph'$.

Solution. On forme $\widehat{\mathscr{E}}$ (ensemble des $\widehat{F}$ pour $F \in \mathscr{E}$) à l'aide de symboles fonctionnels tous distincts et non dans $\mathscr{L}(\mathscr{E})$. Comme $\mathscr{E}$ a un modèle celui-ci s'étend en un modèle de $\widehat{\mathscr{E}}$. Ajoutons à $\mathscr{L}(\mathscr{E})$ un ensemble C de symboles de constantes de cardinal $\aleph'$. Comme $\widehat{\mathscr{E}}$ a un modèle il a un modèle canonique (pour ce nouveau langage) dont le cardinal est évidemment $\aleph'$.

5. On appelle sous-réalisation d'une réalisation d'un langage $\mathscr{L}$, dont l'ensemble de base est E, une réalisation de $\mathscr{L}$ dont l'ensemble de base $E' \subset E$ est tel que $\overline{\varphi}(E'^n) \subset E'$ pour tout $\varphi \in F^n_{\mathscr{L}}$; les valeurs des symboles fonctionnels et relationnels étant les restrictions à E' de leurs valeurs dans la réalisation donnée.

a) Montrer que si $\mathscr{E}$ est un ensemble de formules prénexes purement universelles toute sous-réalisation d'un modèle de $\mathscr{E}$ est un modèle de $\mathscr{E}$.

b) Montrer que si $\mathscr{E}$ est un ensemble de formules prénexes quelconques de cardinal $\aleph \geqslant \aleph_0$, qui a un modèle, il existe une sous-réalisation de ce modèle, dont l'ensemble de base est de cardinal $\leqslant \aleph$, qui est un modèle de $\mathscr{E}$.

Solution. — *a*) Soit F une formule sans quantificateurs, $\overline{F}$ la valeur qu'elle prend dans la réalisation de base $E(\overline{F} \subset E^{V_{\mathscr{L}}})$ et $\overline{\overline{F}}$ la valeur qu'elle prend dans la sous-réalisation de base $E'(\overline{\overline{F}} \subset E'^{V_{\mathscr{L}}} \subset E^{V_{\mathscr{L}}})$.

Alors on a $\overline{\overline{F}} = \overline{F} \cap E'^{V_{\mathscr{L}}}$; c'est clair si F est atomique, et, d'autre part, si F et G satisfont à cette égalité $\neg F$ et $F \vee G$ y satisfont aussi. Soit alors $A = \Lambda x_1 \ldots \Lambda x_n F$ (F sans quantificateurs) une formule de $\mathscr{E}$. Elle est satisfaite par la réalisation de base E et par suite $\overline{F} = E^{V_{\mathscr{L}}}$. Donc $\overline{\overline{F}} = E'^{V_{\mathscr{L}}}$ et par suite la formule A est aussi satisfaite dans la sous-réalisation de base E'.

b) On construit l'ensemble $\widehat{\mathscr{E}}$ à l'aide de symboles fonctionnels tous distincts et non dans $\mathscr{L}(\mathscr{E})$, et on prolonge le modèle donné de $\mathscr{E}$ en un modèle de $\widehat{\mathscr{E}}$. Soit E l'ensemble de base du modèle considéré, et soit T l'ensemble des termes de $\mathscr{L}(\widehat{\mathscr{E}})$. Il est immédiat que le cardinal de T est $\leqslant \aleph$.

On considère un élément quelconque mais fixé, soit δ, de $E^{V_{\mathscr{L}}}$. On en déduit une application $t \to \overline{t}$ de T dans E (telle que $\overline{x} = \delta(x)$ pour chaque variable x, et telle que pour $\varphi \in F^n_{\mathscr{L}(\mathscr{E})}$ on ait

$$\overline{\varphi t_1 \ldots t_n} = \overline{\varphi}(\overline{t}_1, \ldots, \overline{t}_n)\,,$$

où $\overline{\varphi}$ est la valeur prise par φ dans le modèle de $\widehat{\mathscr{E}}$ considéré). Soit E' l'image de T par cette application. Il est évident que E' est de cardinal $\leqslant \aleph$, et que si φ est un symbole fonctionnel à n variables de $\mathscr{L}(\widehat{\mathscr{E}})$ et si $a_1, \ldots, a_n \in E'$, alors $\overline{\varphi}(a_1, \ldots, a_n) \in E'$. Il en résulte qu'il y a une sous-réalisation du modèle considéré de base E'. D'après *a*) cette sous-réalisation satisfait $\widehat{\mathscr{E}}$ et par suite elle satisfait $\mathscr{E}$.

6. *a*) R étant un symbole relationnel à 2 variables montrer en utilisant la méthode p. 22 que la formule $\wedge x \vee y \wedge z\ (Rxy \vee \neg Rxz)$ est un théorème.

b) Donner un exemple de formule sans quantificateur $A(y)$ telle que $\vee y A(y)$ soit un théorème, mais telle qu'aucune formule $A(t)$ n'en soit un quand t décrit l'ensemble des termes du langage de A.

c) Donner un exemple de formule sans quantificateur $A(x, y, z)$ telle que $\wedge x \vee y \wedge z\ A(x, y, z)$ soit un théorème mais telle que pour aucune suite $t_1(x), ..., t_n(x)$ de termes du langage de A ayant x comme seule variable la formule $A(x, t_1(x), z) \vee \cdots \vee A(x, t_n(x), z)$ n'en soit un.

Solution. — *a*) Il est immédiat que cette formule est un théorème : en effet c'est la clôture de $\vee y Rxy \vee \wedge z \neg Rxz$ qui est de la forme $A \vee \neg A$. Si $F = \wedge x \vee y \wedge z(Rxy \vee \neg Rxz)$, on a $\check{F} = \vee y\ [R(a, y) \vee \neg R(a, \varphi y)]$, où a est un symbole de constante, et φ un symbole fonctionnel à une seule variable. Le théorème d'uniformité affirme l'existence de termes $t_1, ..., t_k$ formés avec a, φ et des variables tels que :

$$[R(a, t_1) \vee \neg R(a, \varphi t_1)] \vee \cdots \vee [R(a, t_k) \vee \neg R(a, \varphi t_k)]$$

soit un théorème du calcul propositionnel. Il est immédiat qu'on peut prendre $t_1 = a$; $t_2 = \varphi a$. On obtient la formule

$$R(a, a) \vee \neg R(a, \varphi a) \vee R(a, \varphi a) \vee \neg R(a, \varphi \varphi a)$$

qui est évidemment un théorème du calcul propositionnel.

b) Posons $A(y) = R(a, y) \vee \neg R(a, \varphi y)$. On vient de voir que $\vee y A(y)$ est un théorème. Or si pour un terme t du langage de $A(y)$,

$$R(a, t) \vee \neg R(a, \varphi t)$$

était un théorème ce serait aussi un théorème du calcul propositionnel construit avec $p = R(a, t)$ et $q = R(a, \varphi t)$ ce qui est manifestement faux.

c) Posons $A(x, y, z) = Rxy \vee \neg Rxz$. On a vu que $\wedge x \vee y \wedge z A(x, y, z)$ est un théorème. Or il est immédiat que $A(x, t_1(x), z) \vee \cdots \vee A(x, t_n(x)\ z)$ équivaut à $\neg Rxz \vee R(x, t_1(x)) \vee \cdots \vee R(x, t_n(x))$, qui ne peut être un théorème du calcul propositionnel si aucun des $t_i(x)$ n'est égal à z.

7. On considère une formule F et on construit $\hat{F}$ et $\check{F}$ à l'aide de symboles fonctionnels distincts. Montrer que $\hat{F} \rightarrow \check{F}$ est un théorème. Quelle est la formule d'interpolation ? On pose $F = \wedge x \vee y \wedge z A(x, fy, z)$ où A est un symbole relationnel à 3 variables et f un symbole fonctionnel à une variable. Retrouver la formule d'interpolation pour $\hat{F} \rightarrow \check{F}$ en suivant la démonstration du lemme d'interpolation.

Solution. — On a montré que $\hat{F} \to F$ et $F \to \check{F}$ sont des théorèmes. Il en résulte que $\hat{F} \to \check{F}$ en est un aussi. D'autre part comme $\hat{F}$ et $\check{F}$ ont été formées à l'aide de symboles fonctionnels distincts on a

$$\mathscr{L}(F) \subset \mathscr{L}(\hat{F}) \cap \mathscr{L}(\check{F}).$$

Donc F est une formule d'interpolation.

Si $F = \bigwedge x \bigvee y \bigwedge z A(x, fy, z)$, on a

$$\hat{F} = \bigwedge x \bigwedge z A(x, f\varphi x, z) \qquad \text{et} \qquad \check{F} = \bigvee y A(\alpha, fy, \psi\alpha y),$$

où α, φ et ψ sont des symboles fonctionnels à 0,1 et 2 variables respectivement. On a donc le théorème $\neg \hat{F} \vee \check{F}$ soit

$$\bigvee x \bigvee z \neg A(x, f\varphi x, z) \vee \bigvee y A(\alpha, fy, \psi\alpha y)$$

qu'on peut écrire pour suivre la démonstration du lemme d'interpolation sous la forme $\bigvee x \bigvee z H(x, z) \vee \bigvee y K(y)$.

On vérifie immédiatement que $H(\alpha, \psi(\alpha, \varphi\alpha)) \vee K(\varphi\alpha)$ est un théorème du calcul propositionnel (il s'écrit sous la forme $\neg \mathcal{C} \vee \mathcal{C}$, où $\mathcal{C} = A(\alpha, f\varphi\alpha, \psi\alpha\varphi\alpha)$. La formule d'interpolation pour le calcul propositionnel est $\mathcal{C}$.

On écrit $\mathcal{C} = C(\xi_1, \ldots, \xi_p)$, la formule $C(z_1, \ldots, z_p)$ du texte étant ici $Az_1 z_2 z_3$, avec $\xi_1 = \alpha$, $\xi_2 = f\varphi\alpha$, $\xi_3 = \psi\alpha\varphi\alpha$. On choisit le plus long ξ_i (ici ξ_2) commençant par un symbole fonctionnel commun à $\hat{F}$ et $\check{F}$ et on pose

$$C_2(z_1, z_2, z_3) = C_1(z_1, fz_2, z_3) = A(z_1, fz_2, z_3).$$

On a alors $\xi_1^2 = \alpha$; $\xi_2^2 = \varphi\alpha$; $\xi_3^2 = \psi\alpha\varphi\alpha$ et la suite des C_p s'arrête là. La formule $M(z_1, \ldots, z_q)$ du texte est donc ici $A(z_1, fz_2, z_3)$ et on a $\eta_3 = \alpha$; $\eta_2 = \varphi\alpha$; $\eta_1 = \psi\alpha\varphi\alpha$. La formule d'interpolation cherchée est donc

$$C = Q_1 z_1 Q_2 z_2 Q_3 z_3 A(z_1, fz_2, z_3),$$

avec $Q_1 = \bigwedge$ (car η_1 commence par $\psi \in \mathscr{L}(\check{F})$), $Q_2 = \bigvee$ (car η_2 commence par $\varphi \in \mathscr{L}(\hat{F})$) et $Q_3 = \bigwedge$ (car η_3 commence par $\alpha \in \mathscr{L}(\check{F})$). La formule cherchée est donc $\bigwedge z_1 \bigvee z_2 \bigwedge z_3 A(z_1, fz_2, z_3)$ qui est équivalente à $F = \bigwedge x \bigvee y \bigwedge z A(x, fy, z)$. On retrouve donc la même formule d'interpolation.

8. On dit qu'une formule A est conséquence d'un ensemble $\mathscr{E}$ de formules si toute réalisation qui satisfait $\mathscr{E}$ satisfait aussi A.

a) Montrer que pour que A soit conséquence d'un ensemble fini $\{A_1, \ldots, A_n\}$ il faut et il suffit que $A_1 \wedge \ldots \wedge A_n \to A$ soit un théorème.

b) Montrer que pour que A soit conséquence d'un ensemble $\mathscr{E}$ il faut et il suffit qu'elle soit conséquence d'un sous-ensemble fini de $\mathscr{E}$.

c) Un ensemble $\mathscr{E}$ est dit indépendant si aucune formule de $\mathscr{E}$ n'est conséquence des autres. Montrer que pour que $\mathscr{E}$ soit indépendant il faut et il suffit que tout sous-ensemble fini de $\mathscr{E}$ le soit.

d) Montrer que pour tout ensemble $\mathscr{E}$ fini il y a un sous-ensemble indépendant équivalent, et que pour tout ensemble $\mathscr{E}$ dénombrable il existe un ensemble indépendant équivalent.

Solution. — Démonstrations semblables à celles déjà faites dans le cas du calcul propositionnel.

---

3. CALCUL DES PRÉDICATS AVEC ÉGALITÉ

Résumé

On considère maintenant, parmi les langages étudiés dans le chapitre précédent, ceux qui contiennent le symbole = ; et on ne considère que les réalisations dans lesquelles = représente l'identité. On verra que l'étude de ces réalisations particulières (égalitaires) peut être réduite à la théorie générale du chapitre précédent. Il faut noter que, lorsqu'on impose une réalisation déterminée à un symbole de relation donné, la classe de réalisations ainsi obtenue possède en général une théorie assez différente, cf. les ω-modèles du chapitre 7.

Le principal résultat donné dans le texte consiste en un ensemble commode de conditions nécessaires et suffisantes pour qu'une réalisation donnée soit plongeable dans un modèle d'un ensemble donné de formules. Ces conditions conservent d'ailleurs une signification dans le cas sans égalité. Comme conséquence intéressante, on obtient un résultat général sur les « lois symétrisables » au sens de Bourbaki, et des conditions purement algébriques, c'est-à-dire du premier ordre, qui équivalent à l'existence d'une relation d'ordre compatible avec une structure donnée (exercice 6).

Le résultat sur les plongements constitue un cas particulier d'un résultat général sur l'équivalence entre certains axiomes dits *du second ordre* (ou d'ordre supérieur) et certains ensembles d'axiomes du premier ordre (chapitre 7 où on étudie la notion d'« axiomes du second ordre »). L'exercice 5 fournit un axiome du second ordre qui est équivalent à un ensemble infini d'axiomes du premier ordre (appartenant au même langage que l'axiome considéré), mais n'est équivalent à aucun ensemble fini de tels axiomes, ce qui établit l'existence d'ensembles infinis de formules du premier ordre qui sont construits à partir d'un nombre *fini* de symboles de relations mais ne sont équivalents à aucun de leurs sous-ensembles finis.

Les exercices 1 et 2 établissent, pour les systèmes d'axiomes du premier ordre, certaines propriétés fondamentales de non-catégoricité (même vis-à-vis des réalisations égalitaires). En gros, ni la notion d'ensemble fini, ni celle d'ensemble dénombrable, ni celle de l'ensemble des nombres naturels (N muni de la relation de successeur), ne peut être caractérisée au moyen de formules du premier ordre. On montrera dans le chapitre 7 que les caractérisations habituelles de ces notions (caractérisations dues à Dedekind et Peano) peuvent être mises sous une forme du *second* ordre, ce qui montre qu'il y a des conditions du second ordre qui ne sont équivalentes (au sens d'avoir la même classe de réalisations) à aucun ensemble de formules du premier ordre.

Un langage $\mathscr{L}$ est dit égalitaire si $\mathrm{R}^2_{\mathscr{L}} \neq \phi$ et si on a choisi un élément E de $\mathrm{R}^2_{\mathscr{L}}$ (appelé symbole d'égalité).

Une réalisation du langage égalitaire $\mathscr{L}$, sur l'ensemble de base U sera dite égalitaire si dans cette réalisation $\overline{E}$ est la diagonale de U^2 (ensemble des (x, x) pour $x \in U$).

Une formule A de $\mathscr{L}$ sera appelée *théorème du calcul des prédicats avec égalité* si dans toute réalisation égalitaire de $\mathscr{L}$ on a $\overline{A} = U^{V_{\mathscr{L}}}$ (où U est l'ensemble de base de la réalisation), c'est-à-dire si toute réalisation égalitaire de $\mathscr{L}$ satisfait A.

Etant donné un langage égalitaire $\mathscr{L}$ nous désignerons par $\mathscr{E}_{\mathscr{L}}$ l'ensemble des formules suivantes, appelées axiomes de l'égalité pour le langage $\mathscr{L}$:

1) $\bigwedge x Exx$.

2) Pour chaque $P \in \mathrm{R}^n_{\mathscr{L}}$ (y compris $P = E$) :

$$\bigwedge x_1 \bigwedge x_2 \dots \bigwedge x_n \bigwedge y_1 \dots \bigwedge y_n [Ex_1 y_1 \wedge \cdots \wedge Ex_n y_n \wedge Px_1 \dots x_n \rightarrow Py_1 \dots y_n] .$$

3) Pour chaque $\varphi \in \mathrm{F}^n_{\mathscr{L}}$:

$$\bigwedge x_1 \dots \bigwedge x_n \bigwedge y_1 \dots \bigwedge y_n [Ex_1 y_1 \wedge \cdots \wedge Ex_n y_n \rightarrow E\varphi x_1 \dots x_n, \varphi y_1 \dots y_n] .$$

Il est clair que chaque formule de $\mathscr{E}_{\mathscr{L}}$ est un théorème égalitaire.

Soit $\mathfrak{M}$ une réalisation de $\mathscr{L}$ qui satisfasse $\mathscr{E}_{\mathscr{L}}$. Elle satisfait donc les formules

$$\bigwedge x Exx \quad \text{et} \quad \bigwedge x_1 \bigwedge x_2 \bigwedge y_1 \bigwedge y_2 [Ex_1 y_1 \wedge Ex_2 y_2 \wedge Ex_1 x_2 \rightarrow Ey_1 y_2] ,$$

ce qui montre que $\overline{E}$ (valeur prise par E dans cette réalisation) est le graphe d'une relation d'équivalence sur l'ensemble de base U de $\mathfrak{M}$. D'après les formules 2) de $\mathscr{E}_{\mathscr{L}}$, pour chaque $P \in R^n$, $\overline{P}$ est saturé vis-à-vis de la relation d'équivalence $\overline{E}$ (c'est-à-dire, si $(a_1, \dots, a_n) \in \overline{P}$ et si $a_1 \sim b_1, \dots, a_n \sim b_n$ par la relation $\overline{E}$ alors $(b_1, \dots, b_n) \in \overline{P}$). Désignons alors par $\mathfrak{M}'$ la réalisation égalitaire suivante de $\mathscr{L}$: l'ensemble de base est $U' = U/\overline{E}$ (quotient de U par la relation d'équivalence $\overline{E}$). Pour chaque $P \in \mathrm{R}^n_{\mathscr{L}}$, la valeur $\overline{\overline{P}}$ prise par P dans $\mathfrak{M}'$ est $\overline{\overline{P}} = \overline{P}/\overline{E}$. Pour chaque $\varphi \in \mathrm{F}^n_{\mathscr{L}}$, la valeur $\overline{\overline{\varphi}}$ prise par φ est définie par passage au quotient à partir de $\overline{\varphi}$ (ce qui est possible puisque $\mathfrak{M}$ satisfait les formules 3) de $\mathscr{E}_{\mathscr{L}}$ qui montrent que $\overline{\varphi}$ est compatible avec la relation d'équivalence $\overline{E}$).

LEMME. — *Pour chaque formule A de $\mathscr{L}$, $\overline{A}$ (valeur prise par A dans la réalisation $\mathfrak{M}$) est saturée vis-à-vis de la relation d'équivalence $\overline{E}$ et on a $\overline{\overline{A}} = \overline{A}/\overline{E}$.*

Par récurrence sur la longueur de A : c'est immédiat si A est atomique ou si $A = \neg B$ ou $\vee BC$, B et C étant supposées satisfaire au lemme (on a alors $\overline{A} = \complement \overline{B}$ par exemple et $\overline{\overline{A}} = \complement \overline{\overline{B}}$; comme $\overline{B}$ est saturée $\complement \overline{B}$ l'est aussi et $\complement \overline{\overline{B}} = \complement \overline{B}/\overline{E}$).

Si $A = \bigvee x B$, B satisfaisant au lemme, soient $x, x_1, \dots, x_n$ les variables libres de B. $\overline{A}$ est (au produit près par $U^{V_{\mathscr{L}} - \{x_1, \dots, x_n\}}$) l'ensemble des

$$(a_1, \dots, a_n) \in U^{\{x_1, \dots, x_n\}}$$

tels qu'il existe un $a \in U$ tel que $(a, a_1, ..., a_n) \in \bar{B}$. Or si

$$a'_1 \sim a_1, ..., a'_n \sim a_n$$

suivant la relation $\bar{E}$, comme $\bar{B}$ est saturée par hypothèse, on a $(a, a'_1, ..., a'_n) \in \bar{B}$ et par suite $(a'_1, ..., a'_n) \in \bar{A}$ ce qui montre que $\bar{A}$ est aussi saturé. $\bar{\bar{A}}$ est l'ensemble des $(\alpha_1, ..., \alpha_n) \in U'^{\{x_1, ..., x_n\}}$ tels qu'il existe $\alpha \in U'$ tel que $(\alpha, \alpha_1, ..., \alpha_n) \in \bar{\bar{B}}$. Soient $a, a_1, ..., a_n$ des éléments de U, dont les classes suivant $\bar{E}$ sont α, $\alpha_1, ..., \alpha_n$. Puisque $\bar{B}$ satisfait au lemme, $(a, a_1, ..., a_n) \in \bar{B}$ donc $(a_1, ..., a_n) \in \bar{A}$ et par suite $\bar{\bar{A}} = \bar{A}/\bar{E}$. C. q. f. d.

THÉORÈME : *Pour qu'un ensemble $\mathscr{A}$ de formules de $\mathscr{L}$ ait un modèle égalitaire, il faut et il suffit que $(\mathscr{E}_{\mathscr{L}}, \mathscr{A})$ ait un modèle.*

La condition est évidemment nécessaire, toute formule de $\mathscr{E}_{\mathscr{L}}$ étant un théorème égalitaire.

Inversement si $(\mathscr{E}_{\mathscr{L}}, \mathscr{A})$ a un modèle $\mathfrak{M}$, dans la réalisation égalitaire $\mathfrak{M}'$ déduite de $\mathfrak{M}$ comme ci-dessus on a $\bar{\bar{A}} = \bar{A}/\bar{E}$ pour toute formule A. La réalisation $\mathfrak{M}$ satisfaisant chaque formule A de $\mathscr{A}$, la réalisation $\mathfrak{M}'$ satisfait aussi chaque formule A de $\mathscr{A}$. C. q. f. d.

COROLLAIRE 1. — *Tout ensemble dénombrable $\mathscr{A}$ de formules de $\mathscr{L}$ qui a un modèle égalitaire, a un modèle égalitaire dénombrable ou fini.*

Car $\mathscr{E}_{\mathscr{L}(\mathscr{A})}$ est aussi dénombrable, donc $(\mathscr{E}_{\mathscr{L}(\mathscr{A})}, \mathscr{A})$ a un modèle dénombrable. L'ensemble de base du modèle égalitaire de $\mathscr{A}$ déduit de ce modèle est le quotient de l'ensemble de base de ce modèle par une relation d'équivalence (voir plus haut). Il en résulte qu'il est dénombrable ou fini.

COROLLAIRE 2. — *Pour qu'une formule A soit un théorème égalitaire, il faut et il suffit qu'elle soit conséquence de $\mathscr{E}_{\mathscr{L}(A)}$.*

La condition est évidemment suffisante. Elle est nécessaire car si A est un théorème égalitaire, $\neg A$ n'a pas de modèle égalitaire, donc d'après le théorème précédent $(\mathscr{E}_{\mathscr{L}(A)}, \neg A)$ n'a pas de modèle du tout, ce qui montre que A est conséquence de $\mathscr{E}_{\mathscr{L}(A)}$.

THÉORÈME DE FINITUDE. — *Pour qu'un ensemble $\mathscr{A}$ de formules de $\mathscr{L}$ ait un modèle égalitaire, il faut et il suffit que tout sous-ensemble fini de $\mathscr{A}$ en ait un.*

La condition est évidemment nécessaire. Elle est suffisante car alors tout sous-ensemble fini de $(\mathscr{E}_{\mathscr{L}}, \mathscr{A})$ a un modèle, donc $(\mathscr{E}_{\mathscr{L}}, A)$ a un modèle et par suite $\mathscr{A}$ a un modèle égalitaire.

LEMME D'INTERPOLATION. — *Si $A \to B$ est un théorème égalitaire, il existe une formule C telle que $\mathscr{L}(C) \subset \mathscr{L}(A) \cap \mathscr{L}(B)$ et telle que $A \to C$ et $C \to B$ soient des théorèmes égalitaires.*

Par abus de langage désignons aussi par $\mathscr{E}_{\mathscr{L}(A)}$ la conjonction des formules de $\mathscr{E}_{\mathscr{L}(A)}$ (qui sont en nombre fini). Par hypothèse $A \to B$ est conséquence de $\mathscr{E}_{\mathscr{L}(A)} \wedge \mathscr{E}_{\mathscr{L}(B)}$ (d'après le corollaire ci-dessus). Donc

$$\mathscr{E}_{\mathscr{L}(A)} \wedge \mathscr{E}_{\mathscr{L}(B)} \to (A \to B)$$

est un théorème et par suite aussi

$$\mathscr{E}_{\mathscr{L}(A)} \wedge A \to (\mathscr{E}_{\mathscr{L}(B)} \to B)\,.$$

D'après le lemme d'interpolation il y a une formule C telle que

$$\mathscr{L}(C) \subset \mathscr{L}(A) \cap \mathscr{L}(B)$$

et telle que $\mathscr{E}_{\mathscr{L}(A)} \wedge A \to C$ et $C \to (\mathscr{E}_{\mathscr{L}(B)} \to B)$ soient des théorèmes. Donc $\mathscr{E}_{\mathscr{L}(A)} \to (A \to C)$ et $\mathscr{E}_{\mathscr{L}(B)} \to (C \to B)$ sont des théorèmes ce qui montre que $A \to C$ et $C \to B$ sont des théorèmes égalitaires. (Cf. Ex. 4 du Ch. 5).

THÉORÈME DE DÉFINISSABILITÉ I. — *Soient A une formule, R un symbole relationnel à n variables de $\mathscr{L}(A)$, A' la formule obtenue en substituant à R dans A un symbole relationnel R' à n variables non dans $\mathscr{L}(A)$. Alors si*

$$A \wedge A' \to (Rx_1 \ldots x_n \to R'\,x_1 \ldots x_n)$$

est un théorème égalitaire, il y a une formule F, telle que $\mathscr{L}(F) \subset \mathscr{L}(A)$ et $R \notin \mathscr{L}(F)$ telle que $A \to (F \leftrightarrow Rx_1 \ldots x_n)$ soit un théorème égalitaire.

Même démonstration que plus haut à partir du lemme d'interpolation.

THÉORÈME DE DÉFINISSABILITÉ II. — *Soient A une formule, φ un symbole fonctionnel à n variables de $\mathscr{L}(A)$, A' la formule obtenue en substituant à φ dans A, un symbole fonctionnel à n variables φ' non dans $\mathscr{L}(A)$. Alors si*

$$A \wedge A' \to (\varphi x_1 \ldots x_n = \varphi'\,x_1 \ldots x_n)$$

est un théorème égalitaire, il y a une formule F de $\mathscr{L}(A)$ telle que $\varphi \notin \mathscr{L}(F)$ et telle que $A \to (F \leftrightarrow y = \varphi x_1 \ldots x_n)$ soit un théorème égalitaire.

(Dans l'énoncé de ce théorème on a écrit $u = v$ au lieu de Euv.)

Car $A \wedge A' \wedge (y = \varphi x_1 \ldots x_n) \to (y = \varphi'\,x_1 \ldots x_n)$ est un théorème égalitaire. Donc $A \wedge (y = \varphi x_1 \ldots x_n) \to (A' \to y = \varphi'\,x_1 \ldots x_n)$ en est un aussi. D'où le résultat cherché en appliquant le lemme d'interpolation à cette formule.

On a encore les théorèmes suivants qui sont des conséquences immédiates de leurs analogues au chapitre précédent :

THÉORÈME. — *Pour toute formule prénexe F il existe une formule prénexe $\hat{F}$ purement universelle et une formule prénexe $\check{F}$ purement existentielle telles que :*

a) *$\hat{F} \to F$ et $F \to \check{F}$ soient deux théorèmes égalitaires.*

b) *Toute réalisation de $\mathscr{L}(F)$ se prolonge à $\mathscr{L}(\hat{F})$ et à $\mathscr{L}(\check{F})$ de façon que $\overline{F} = \overline{\hat{F}}$ et $\overline{F} = \overline{\check{F}}$.*

THÉORÈME D'UNIFORMITÉ. — *Pour que la formule* $\forall x_1 \dots \forall x_m A(x_1, \dots, x_m)$ (*A étant sans quantificateurs*) *soit un théorème égalitaire, il faut et il suffit qu'il existe des termes* $t_1^i, \dots, t_m^i$ $(1 \leqslant i \leqslant k)$ *tels que la formule* $\bigvee_{i=1}^{k} A(t_1^i, \dots, t_m^i)$ *soit conséquence* (*au sens du calcul propositionnel construit sur les formules atomiques de* $\mathscr{L}(A)$) *de l'ensemble suivant* :

1) *Pour chaque terme* $t \in \mathscr{L}(A)$, $t = t$.

2) *Pour chaque symbole relationnel P à n variables de* $\mathscr{L}(A)$ *et chaque*

$$(t_1, \dots, t_n) \in (T_{\mathscr{L}(A)})^n \quad et \quad (t'_1, \dots, t'_n) \in (T_{\mathscr{L}(A)})^n :$$

$$t_1 = t'_1 \wedge \cdots \wedge t_n = t'_n \wedge Pt_1 \dots t_n \to Pt'_1 \dots t'_n .$$

3) *Pour chaque symbole fonctionnel φ à n variables de* $\mathscr{L}(A)$ *et chaque*

$$(t_1, \dots, t_n) \quad et \quad (t'_1, \dots, t'_n) \in (T_{\mathscr{L}(A)})^n :$$

$$t_1 = t'_1 \wedge \cdots \wedge t_n = t'_n \to \varphi t_1 \dots t_n = \varphi t'_1 \dots t'_n .$$

Il suffit d'appliquer le théorème d'uniformité à la formule $\neg\, \mathscr{E}_{\mathscr{L}(A)} \vee A$.

Extensions d'une réalisation.

Etant donnée une réalisation $\mathfrak{M}$ du langage $\mathscr{L}$, d'ensemble de base U, on appelle *extension* de $\mathfrak{M}$, toute réalisation $\mathfrak{M}'$ de $\mathscr{L}$ satisfaisant aux conditions suivantes :

a) L'ensemble de base U' de $\mathfrak{M}'$ contient U.

b) Pour chaque symbole relationnel R de $\mathscr{L}$, à n variables si $\overline{R}$ et $\overline{\overline{R}}$ sont les valeurs qu'il prend dans $\mathfrak{M}$ et $\mathfrak{M}'$ on a $\overline{R} = \overline{\overline{R}} \cap U^n$.

c) Pour chaque symbole fonctionnel φ de $\mathscr{L}$ à n variables, si $\overline{\varphi}$ et $\overline{\overline{\varphi}}$ sont les valeurs qu'il prend dans $\mathfrak{M}$ et $\mathfrak{M}'$, $\overline{\varphi}$ est la restriction de $\overline{\overline{\varphi}}$ à U^n.

LEMME. — *Si $\mathfrak{M}'$ est une extension de $\mathfrak{M}$, pour toute formule F de $\mathscr{L}$ sans quantificateur, si $\overline{F}$ et $\overline{\overline{F}}$ sont les valeurs qu'elle prend dans $\mathfrak{M}$ et $\mathfrak{M}'$, on a*

$$\overline{F} = \overline{\overline{F}} \cap U^{V_{\mathscr{L}}} .$$

Par récurrence sur la longueur de F. Si F est atomique on a $F = Rt_1 \dots t_n$. Soient $x_1, \dots, x_k$ les variables de F. $\overline{F}$ est l'ensemble des $(a_1, \dots, a_k) \in U^{\{x_1, \dots, x_k\}}$ tels que $(\overline{t}_1, \dots, \overline{t}_n) \in \overline{R} = \overline{\overline{R}} \cap U^n$. Comme sur $U^{\{x_1, \dots, x_k\}}$ on a $\overline{t}_i = \overline{\overline{t}}_i$ $(1 \leqslant i \leqslant n)$, on a bien $\overline{F} = \overline{\overline{F}} \cap U^{\{x_1, \dots, x_k\}}$. D'autre part il est clair que si F et G satisfont au lemme $\neg F$ et $\vee FG$ y satisfont aussi $(\overline{\neg F} = \complement \overline{F}\, ;\ \overline{\vee FG} = \overline{F} \cup \overline{G})$.

C. q. f. d.

THÉORÈME. — *Si $\mathfrak{M}'$ est une extension de $\mathfrak{M}$ toute formule close purement universelle de $\mathscr{L}$ satisfaite dans $\mathfrak{M}'$ l'est aussi dans $\mathfrak{M}$.*

Car si $\wedge x_1 \dots \wedge x_n A(x_1, \dots, x_n)$ est satisfaite dans $\mathfrak{M}'$, A étant sans quantificateurs, la valeur de A dans $\mathfrak{M}'$ est $U'^{V_{\mathscr{L}}}$, donc sa valeur dans $\mathfrak{M}$ est $U^{V_{\mathscr{L}}}$ d'après le lemme. Par suite A est satisfaite dans $\mathfrak{M}$.

Dans la suite de ce chapitre les langages et les réalisations considérés sont toujours supposés égalitaires.

Etant donnée une réalisation $\mathfrak{M}$ d'un langage égalitaire $\mathscr{L}$, d'ensemble de base U, on appelle diagramme de $\mathfrak{M}$ l'ensemble $D_{\mathfrak{M}}$ des formules suivantes du langage $\mathscr{L}'$ obtenu en ajoutant à $\mathscr{L}$ les éléments de U comme symboles de constantes (on suppose $U \cap F^0_{\mathscr{L}} = \phi$) :

a) pour chaque $R \in \mathrm{R}^n_{\mathscr{L}}$ et pour chaque $(a_1, \dots, a_n) \in U^n$ la formule $Ra_1 \dots a_n$ ou $\neg Ra_1 \dots a_n$ suivant que $(a_1, \dots, a_n) \in \overline{R}$ ou $(a_1, \dots, a_n) \notin \overline{R}$;

b) pour chaque $\varphi \in \mathrm{F}^n_{\mathscr{L}}$ et pour chaque $(a, a_1, \dots, a_n) \in U^{n+1}$, la formule $a = \varphi a_1 \dots a_n$ ou $a \neq \varphi a_1 \dots a_n$ suivant que $a = \overline{\varphi}(a_1, \dots, a_n)$ ou $a \neq \overline{\varphi}(a_1, \dots, a_n)$ dans $\mathfrak{M}$. En particulier $D_{\mathfrak{M}}$ contient pour tout couple (a, b) de U^2 la formule $a = b$ ou $a \neq b$ suivant qu'on a effectivement $a = b$ ou $a \neq b$.

THÉORÈME. — *Pour qu'une réalisation $\mathfrak{M}'$ de $\mathscr{L}$ soit une extension de $\mathfrak{M}$ (à un isomorphisme près), il faut et il suffit que $\mathfrak{M}'$ s'étende à $\mathscr{L}'$ de façon à satisfaire $D_{\mathfrak{M}}$.*

En effet pour que $\mathfrak{M}'$ ait une sous-réalisation isomorphe à $\mathfrak{M}$, il faut et il suffit qu'il existe une application bi-univoque de U dans U' compatible avec les valeurs des symboles relationnels et fonctionnels de $\mathscr{L}$ dans les deux réalisations. Or se donner une telle application revient à étendre $\mathfrak{M}'$ à $\mathscr{L}'$ de façon à satisfaire $D_{\mathfrak{M}}$.

THÉORÈME DE PLONGEMENT. — *Pour qu'une réalisation $\mathfrak{M}$ d'un langage $\mathscr{L}_0$ ait une extension qui soit un modèle d'un ensemble donné $\mathscr{A}$ de formules d'un langage $\mathscr{L}_1$, il faut et il suffit que $\mathfrak{M}$ satisfasse toutes les formules purement universelles de $\mathscr{L}_0$, qui sont conséquences de $\mathscr{A}$.*

La condition est évidemment nécessaire : en effet si $\mathfrak{M}'$ est une extension de $\mathfrak{M}$, $\mathfrak{M}$ satisfait toutes les formules purement universelles satisfaites par $\mathfrak{M}'$.

Inversement, s'il n'existe aucune extension de $\mathfrak{M}$ qui satisfasse $\mathscr{A}$, l'ensemble $(\mathscr{A}, D_{\mathfrak{M}})$ est contradictoire d'après le théorème précédent. Par suite il existe un sous-ensemble fini Δ de $D_{\mathfrak{M}}$ tel que $(\mathscr{A}, \Delta)$ soit contradictoire (théorème de finitude). U désignant l'ensemble de base de $\mathfrak{M}$, soient $a_1, \dots, a_n$ les éléments de U apparaissant dans Δ et soit $F(a_1, \dots, a_n)$ la conjonction des formules de Δ, $F(x_1, \dots, x_n)$ étant une formule sans quantificateurs de $\mathscr{L}_0$. Il est clair $F(a_1, \dots, a_n)$ est satisfaite par $\mathfrak{M}$ si on pose $\overline{a}_1 = a_1, \dots, \overline{a}_n = a_n$. Il en résulte que

$$\vee x_1 \dots \vee x_n F(x_1, \dots, x_n)$$

est satisfaite dans $\mathfrak{M}$. Or $(\mathscr{A}, F(a_1, \dots, a_n))$ est contradictoire, donc $\neg F(a_1, \dots, a_n)$ est conséquence de $\mathscr{A}$. Comme $a_1, \dots, a_n$ sont des symboles de constantes non

dans $\mathscr{L}_1$, donc n'apparaissant pas dans $\mathscr{A}$, $\bigwedge x_1 \dots \bigwedge x_n \neg F(x_1, \dots, x_n)$ est conséquence de $\mathscr{A}$. On a donc trouvé une formule purement universelle de $\mathscr{L}_0$ conséquence de $\mathscr{A}$ et non satisfaite par $\mathfrak{M}$. C. q. f. d.

Application. — On prend le langage $\mathscr{L}_0$ constitué par un seul symbole fonctionnel à 2 variables : $\times$ ($\times xy$ étant noté xy). Il existe un ensemble $\mathscr{G}$ (évidemment dénombrable) de formules closes purement universelles de $\mathscr{L}_0$, tel que, pour qu'un monoïde se plonge dans un groupe, il faut et il suffit qu'il satisfasse $\mathscr{G}$.

En effet un monoïde M est une réalisation de $\mathscr{L}_0$. Si on désigne par $\mathscr{A}$ l'ensemble des formules suivantes du langage $\mathscr{L}_1$ constitué par : $\times$ (symbole fonctionnel à 2 variables), $^{-1}$ (symbole fonctionnel à 1 variable), e (symbole de constante) :

$$\bigwedge x \bigwedge y \bigwedge z[x(yz) = (xy)z] ; \quad \bigwedge x[x.e = e.x = x] ; \quad \bigwedge x[x.x^{-1} = e] ,$$

le théorème précédent donne l'existence de l'ensemble $\mathscr{G}$.

Remarque. — Une des formules de $\mathscr{G}$ est la règle de simplification :

$$\bigwedge x \bigwedge y \bigwedge u \bigwedge v[uxv = uyv \rightarrow x = y] .$$

Cette formule suffit si le monoïde M est commutatif.

Etant donnée une réalisation $\mathfrak{M}$ d'un langage $\mathscr{L}$, d'ensemble de base E, pour qu'un sous-ensemble F de E soit l'ensemble de base d'une sous-réalisation $\mathfrak{M}'$ de $\mathfrak{M}$, il faut et il suffit que pour tout symbole fonctionnel φ à n variables de $\mathscr{L}$, et pour tout élément $(a_1, \dots, a_n)$ de F^n, $\overline{\varphi}(a_1, \dots, a_n)$ soit dans F ($\overline{\varphi}$ étant la valeur prise par φ dans la réalisation $\mathfrak{M}$). Il est clair que toute intersection de sous-ensembles de E ayant cette propriété la possède aussi. On peut donc donner la définition suivante :

Pour tout sous-ensemble M de E, *la sous-réalisation* $\mathfrak{M}'$ de $\mathfrak{M}$ *engendrée par* M est par définition la sous-réalisation dont l'ensemble de base est le plus petit sous-ensemble de E contenant M et ayant la propriété ci-dessus. Le théorème suivant généralise les exercices 3 et 4 du chapitre 1.

THÉORÈME. — *Pour qu'une réalisation $\mathfrak{M}$ d'un langage $\mathscr{L}_0$ ait une extension qui soit un modèle d'un ensemble donné $\mathscr{A}$ de formules d'un langage $\mathscr{L}_1$ il faut et il suffit que toute sous-réalisation de $\mathfrak{M}$ engendrée par un ensemble fini ait une telle extension.*

Il est clair que la condition est nécessaire, une extension de $\mathfrak{M}$ étant évidemment une extension de chaque sous-réalisation de $\mathfrak{M}$.

Inversement soit $\mathscr{B}$ l'ensemble des formules purement universelles de $\mathscr{L}_0$ qui sont conséquences de $\mathscr{A}$. D'après le théorème de plongement, si $\mathfrak{M}$ n'a pas d'extension qui soit un modèle de $\mathscr{A}$, il y a une formule de $\mathscr{B}$ que $\mathfrak{M}$ ne satisfait pas ; soit $F = \bigwedge x_1 \dots \bigwedge x_k G(x_1, \dots, x_k)$ cette formule, $G(x_1, \dots, x_k)$ étant sans

quantificateurs. Soit $\overline{G}$ la valeur prise par G dans $\mathfrak{M}$. Il existe donc $a_1, ..., a_k \in E$ (ensemble de base de $\mathfrak{M}$) tels que $(a_1, ..., a_k) \notin \overline{G}$. Soit $\mathfrak{M}'$ la sous-réalisation de $\mathfrak{M}$ engendrée par $a_1, ..., a_k$, E' son ensemble de base et $\overline{\overline{G}}$ la valeur prise par G dans $\mathfrak{M}'$. Comme G est sans quantificateurs on a $\overline{\overline{G}} = \overline{G} \cap E'^{\{x_1,...,x_k\}}$. Par suite $(a_1, ..., a_k) \notin \overline{\overline{G}}$ et $\mathfrak{M}'$ ne satisfait pas F. Il en résulte que $\mathfrak{M}'$ n'a pas d'extension satisfaisant $\mathscr{A}$. C. q. f. d.

D'autres exemples d'application sont donnés en exercice.

EXERCICES

Dans ces exercices le symbole d'égalité sera noté $=$ (et non E) et $= xy$ sera écrit $x = y$.

1. Deux réalisations $\mathfrak{M}$ et $\mathfrak{M}'$ d'ensembles de base U et U' d'un langage $\mathscr{L}$ sont dites isomorphes s'il existe une bijection de U sur U' soit φ telle que:

$$\text{pour tout } R \in \mathrm{R}^n_{\mathscr{L}} \text{ on ait } \overline{\overline{R}} = \varphi(\overline{R})$$

(où $\overline{R}$ est la valeur de R dans la réalisation $\mathfrak{M}$ et $\overline{\overline{R}}$ sa valeur dans $\mathfrak{M}'$)

$$\text{pour tout } f \in \mathrm{F}^n_{\mathscr{L}} \text{ on ait } \overline{\overline{f}} = \varphi(\overline{f}) .$$

Un ensemble $\mathscr{A}$ de formules de $\mathscr{L}$ est dit catégorique vis-à-vis d'une classe de réalisations de $\mathscr{L}$ si tous les modèles de $\mathscr{A}$ tirés de cette classe sont isomorphes.

a) Montrer que si un ensemble $\mathscr{A}$ de formules est catégorique vis-à-vis de la classe de toutes les réalisations de $\mathscr{L}$, il n'a pas de modèle (on dit qu'il est contradictoire).

b) Montrer que si $\mathscr{A}$ est catégorique vis-à-vis de la classe des réalisations égalitaires, tout modèle égalitaire de $\mathscr{A}$ a un nombre fini (évidemment fixe) d'éléments.

Solution. – *a*) Soit $\mathscr{A}$ un ensemble de formules ayant un modèle. Si $\aleph$ est le cardinal de ce modèle, on va voir que $\mathscr{A}$ a aussi un modèle de cardinal $\aleph' > \aleph$ ce qui montre que $\mathscr{A}$ n'est pas catégorique. Pour cela formons $\widehat{\mathscr{A}}$ (ensemble des $\widehat{A}$ pour $A \in \mathscr{A}$) à l'aide de symboles fonctionnels distincts non dans $\mathscr{L}(\mathscr{A})$. Soit $\mathscr{L}'$ le langage obtenu en ajoutant à $\mathscr{L}(\widehat{\mathscr{A}})$ un ensemble de symboles de constantes de cardinal $\aleph'' > \aleph$. $\mathscr{A}$ ayant un modèle, $\widehat{\mathscr{A}}$ en a un aussi, donc $\mathscr{A}'$ a un modèle canonique vis-à-vis de $\mathscr{L}'$ (c'est-à-dire dont l'ensemble de base est $T_{\mathscr{L}'}$). Ce modèle a un cardinal $\aleph' \geqslant \aleph''$ donc $\aleph' > \aleph$.

b) Soit $\mathscr{A}$ un ensemble de formules du langage égalitaire $\mathscr{L}$, ayant un modèle égalitaire infini de cardinal $\aleph$. On va voir que $\mathscr{A}$ a un modèle égalitaire de cardinal $> \aleph$. Pour cela ajoutons à $\mathscr{L}(\mathscr{A})$ un ensemble C de symboles de constantes de cardinal $> \aleph$ et soit $\mathscr{B}$ l'ensemble des formules obtenues en ajoutant à $\mathscr{A}$ toutes les formules $a \neq b$ pour a, b éléments distincts de C. Il est clair que tout sous-ensemble fini de $\mathscr{B}$ a un modèle égalitaire (le modèle donné de $\mathscr{A}$ puisque celui-ci est infini). Donc $\mathscr{B}$ tout entier a un modèle égalitaire. Celui-ci a évidemment un cardinal $\geqslant$ à celui de C donc $> \aleph$.

2. On considère le langage égalitaire $\mathscr{L}$ suivant : le seul symbole relationnel de $\mathscr{L}$ est $=$; un symbole de constante : 0 ; un symbole fonctionnel à 1 variable : s (lire « successeur ») ; deux symboles fonctionnels à 2 variables $+$ et $\times$. Etant donnés deux termes t et t', $+tt'$ et $\times tt'$ seront notés $t + t'$ et $t \times t'$. On appelle réalisation standard de $\mathscr{L}$, la réalisation égalitaire de $\mathscr{L}$ dans laquelle l'ensemble de base est **N** (ensemble des entiers $\geqslant 0$) et où les symboles 0, s, $+$, $\times$, prennent leurs valeurs naturelles sur **N** de 0, successeur, addition, multiplication.

On considère l'ensemble $\mathscr{A}$ des formules suivantes de $\mathscr{L}$:

$$\wedge x(sx \neq 0)\,; \quad \wedge x \wedge y(sx = sy \rightarrow x = y)\,; \quad \wedge x \vee y(x = 0 \vee x = sy).$$

$$\wedge x(x + 0 = x)\,; \quad \wedge x \wedge y(s(x + y) = x + sy).$$

$$\wedge x(x \times 0 = 0)\,; \quad \wedge x \wedge y(x \times sy = x \times y + x).$$

a) Montrer que la réalisation standard de $\mathscr{L}$ est un modèle égalitaire de $\mathscr{A}$ (le modèle standard de $\mathscr{A}$) et que tout modèle égalitaire de $\mathscr{A}$ a comme sous-modèle le modèle standard (à un isomorphisme près). Les éléments de ce sous-modèle (c'est-à-dire les valeurs prises par les termes 0, $s0$, $ss0$,...) sont appelés nombres naturels du modèle.

b) Montrer que pour tout ensemble $\mathscr{B}$ de formules de $\mathscr{L}$ contenant $\mathscr{A}$ et possédant un modèle, il n'y a aucune formule $A(x)$ de $\mathscr{L}$ à une seule variable libre dont la valeur dans *tout* modèle de $\mathscr{B}$ soit l'ensemble des nombres naturels de ce modèle.

c) Déduire de *b*) que pour tout ensemble dénombrable $\mathscr{B}$ de formules de $\mathscr{L}$ contenant $\mathscr{A}$ (qui a un modèle) il existe des modèles égalitaires dénombrables non standards (en particulier que $\mathscr{A}$ n'est pas catégorique vis-à-vis de la classe des modèles égalitaires dénombrables).

d) [Amélioration de *b*)]. Le système d'axiomes dit « arithmétique du premier ordre » est obtenu en ajoutant à $\mathscr{A}$ l'ensemble (dénombrable) des formules suivantes : pour chaque formule $A(x)$ de $\mathscr{L}$ ayant les variables libres $x, x_1, ..., x_k$ on ajoute la formule :

$$\wedge x_1 \dots \wedge x_k[(A(0) \wedge \wedge x[A(x) \rightarrow A(sx)]) \rightarrow \wedge x\, A(x)]\,.$$

L'ensemble de ces formules représente le principe de récurrence appliqué aux propriétés définissables en langage $\mathscr{L}$. Montrer que pour toute formule $A(x)$ de $\mathscr{L}$ à une seule variable libre et pour tout modèle $\mathfrak{M}$ non standard des axiomes de l'arithmétique du premier ordre la valeur $\overline{A(x)}$ prise par $A(x)$ dans $\mathfrak{M}$ n'est pas l'ensemble des nombres naturels de $\mathfrak{M}$.

Solution. — *a*) Le fait que la réalisation standard satisfait $\mathscr{A}$ est évident. Inversement si $\mathfrak{M}$ est un modèle égalitaire de $\mathscr{A}$ les 3 premières formules de $\mathscr{A}$ entraînent que les valeurs prises dans $\mathfrak{M}$ par les termes de la forme $s^n 0$ forment un ensemble isomorphe à N par l'application $\overline{s^n 0} \to n$ sur lequel 0 et s ont leur valeur naturelle. Les autres formules de $\mathscr{A}$ entraînent immédiatement que $+$ et $\times$ ont leur valeur d'addition et de multiplication sur cet ensemble. Cet ensemble qui est un sous-ensemble de $\mathfrak{M}$ clos par $\bar{s}$, $\bar{+}$, $\bar{\times}$ est un sous-modèle de $\mathfrak{M}$.

b) Ajoutons un symbole de constante a à $\mathscr{L}$ et considérons l'ensemble des formules $A(a)$, $a \neq 0$, $a \neq s\,0, \ldots, a \neq s^n 0$ pour $n = 1, 2, \ldots$, où $A(x)$ est une formule de $\mathscr{L}$ à une variable libre. Si la valeur prise par $A(x)$ dans tout modèle de $\mathscr{B}$ est l'ensemble des nombres naturels, chaque sous-ensemble fini de cet ensemble de formules a un modèle qui satisfait $\mathscr{B}$ (il suffit de donner comme valeur à a un nombre naturel assez grand). Donc l'ensemble tout entier en a un et, dans ce modèle de $\mathscr{B}$, $A(x)$ est satisfaite par un élément (valeur de a) qui n'est pas un nombre naturel.

c) Prenons pour $A(x)$ dans *b*) la formule $x = x$. Le modèle égalitaire qu'on définit ainsi contient le modèle standard comme sous-modèle strict (puisque la valeur prise par a est différente de tous les nombres naturels d'après *U*) et ne lui est pas isomorphe.

d) Si $\overline{\neg A(x)}$ est l'ensemble vide, $\overline{A(x)}$ contient des éléments non standards puisque $\mathfrak{M}$ est non standard par hypothèse. Si $\overline{\neg A(x)}$ n'est pas vide, comme

$$(A(0) \wedge \bigwedge y[A(y) \to A(sy)]) \to \bigwedge x A(x)$$

équivaut à

$$\bigwedge x[\neg A(x) \to (\neg A(0) \vee \bigvee y[\neg A(sy) \wedge A(y)])] ;$$

ou bien $\bar{0} \notin \overline{A(x)}$, ou bien il existe un $\bar{y}$ non standard $\in \overline{A(x)}$ ou bien il existe un nombre naturel $\bar{y}$ de $\mathfrak{M}$ tel que $\bar{y} \in \overline{A(x)}$ et $\overline{sy} \notin \overline{A(x)}$. Dans chacun de ces cas, $\overline{A(x)}$ n'est pas l'ensemble des nombres naturels de $\mathfrak{M}$.

On voit donc pourquoi les axiomes de Peano sont catégoriques tandis que les axiomes de l'arithmétique du premier ordre ne le sont pas. Les axiomes de Peano exigent que le principe de récurrence puisse être appliqué à toute propriété des éléments de base de la réalisation (de $\mathscr{A}$) considérée, en particulier à la propriété d'être un nombre naturel de cette réalisation ; or cette dernière propriété n'est définissable au moyen du langage $\mathscr{L}$ dans aucune réalisation de $\mathscr{L}$ à l'exception de la réalisation standard.

3. On considère le langage $\mathscr{L}$ suivant : le seul symbole relationnel est $=$; deux symboles de constantes 0, 1 ; deux symboles fonctionnels à deux variables $+$, $\times$. Montrer que pour toute formule A de $\mathscr{L}$ qui est satisfaite dans tous les corps commutatifs de caractéristique 0, il y a un entier N tel que A soit satisfaite dans tous les corps commutatifs de caractéristique $p \geqslant N$.

Solution. — Désignons par C l'ensemble des formules suivantes de $\mathscr{L}$:

$\bigwedge x \bigwedge y \bigwedge z[x + (y + z) = (x + y) + z]$; $\bigwedge x \bigwedge y \bigwedge z[x(yz) = (xy)z]$;

$\bigwedge x \bigwedge y(x + y = y + x)$; $\bigwedge x \bigwedge y[xy = yx]$;

$\bigwedge x(x + 0 = x)$; $\bigwedge x[x.1 = x]$;

$\bigwedge x \bigvee y[x + y = 0]$; $\bigwedge x \bigvee y[x = 0 \vee xy = 1]$;

$\bigwedge x \bigwedge y \bigwedge z[x(y + z) = xy + xz]$; $1 \neq 0$.

Il est clair que les modèles égalitaires de C sont les corps commutatifs. Désignons par F_p la formule $1 + \cdots + 1 = 0$, où 1 est répété p fois. Il est clair que tout modèle égalitaire de l'ensemble $(C, \neg F_2, ..., \neg F_p, ...)$ p parcourant l'ensemble des nombres premiers est un corps de caractéristique 0. Il en résulte que si une formule A de $\mathscr{L}$ est vraie dans tout corps de caractéristique 0 elle est conséquence de $(C, \neg F_2, ..., \neg F_p, ...)$. Par suite elle est conséquence d'un sous-ensemble fini $(C, \neg F_2, ..., \neg F_P)$ et elle est donc satisfaite dans tout corps de caractéristique $p > \underline{P}$.

C. q. f. d.

4. (Théorème de Steinitz). On considère un corps commutatif K. Montrer qu'il existe un sur-corps L de K dans lequel tout polynôme à coefficients dans K se décompose en facteurs du premier degré. En déduire l'existence de la clôture algébrique de K.

Solution. — On considère le langage $\mathscr{L}$ de l'exercice 3. Le corps K est une réalisation de $\mathscr{L}$ dont nous désignerons le diagramme par D_K. Il est clair que tout modèle égalitaire de (C, D_K) (où C est l'ensemble de formules défini à l'exercice 3) est un sur-corps de K.

Pour chaque polynôme $P(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$ à coefficients dans K on considère la formule suivante du langage $\mathscr{L}'$ (dans lequel est exprimé le diagramme de K) :

$$\bigvee x_1 ... \bigvee x_n[a_0 + \cdots + a_{n-1} x^{n-1} + x^n = (x + x_1) ... (x + x_n)] .$$

Désignons par $\mathscr{A}$ l'ensemble de ces formules. Pour tout sous-ensemble fini $\mathscr{A}_0$ de $\mathscr{A}$ on sait que $(C, D_K, \mathscr{A}_0)$ a un modèle égalitaire : on sait en effet construire une extension de K (de dimension finie sur K) dans laquelle un

polynôme à coefficients dans K (donc aussi un ensemble fini de tels polynômes) se décompose en facteurs du premier degré. Il en résulte que tout sous-ensemble fini de $(C, D_K, \mathscr{A})$ a un modèle égalitaire. Par suite $(C, D_K, \mathscr{A})$ a un modèle égalitaire, qui est une extension L de K dans laquelle tout polynôme à coefficients dans K se décompose en facteurs de premier degré. En désignant par Ω le sous-corps de L formé des éléments algébriques sur K on voit immédiatement que Ω est la clôture algébrique de K.

5. On considère le langage $\mathscr{L}_0$ constitué par un symbole relationnel P à 2 variables. Montrer qu'il existe un ensemble U de formules purement universelles de $\mathscr{L}_0$ dont la satisfaction est nécessaire et suffisante pour que P puisse être plongé dans un ordre. Donner un tel ensemble U et montrer qu'il n'équivaut à aucun sous-ensemble fini de conséquences de U. Montrer que la satisfaction de U est nécessaire et suffisante pour que P puisse être plongé dans un ordre total.

Solution. — Considérons dans le langage $\mathscr{L}_1$ constitué par deux symboles relationnels à 2 variables : P et $\leqslant$ l'ensemble $\mathscr{A}$ des formules suivantes :

$$\wedge x \wedge y[Pxy \rightarrow x \leqslant y] ; \qquad \wedge x[x \leqslant x] ;$$
$$\wedge x \wedge y[x \leqslant y \wedge y \leqslant z \rightarrow x = y] ;$$
$$\wedge x \wedge y \wedge z[x \leqslant y \wedge y \leqslant z \rightarrow x \leqslant z] .$$

Pour qu'une réalisation $\mathfrak{M}$ de $\mathscr{L}_0$ se plonge dans un modèle de $\mathscr{A}$, il faut et il suffit qu'elle satisfasse l'ensemble U des conséquences purement universelles de $\mathscr{A}$ ne contenant pas $\leqslant$ (théorème de plongement). Or il est clair que c'est une condition nécessaire et suffisante pour que la valeur $\bar{P}$ de P dans $\mathfrak{M}$ puisse être plongée dans un ordre. Il est immédiat que U contient l'ensemble des formules suivantes :

$$F_n = \wedge x_1 \dots \wedge x_n[Px_1 x_2 \wedge Px_2 x_3 \wedge \cdots \wedge Px_{n-1} x_n \wedge Px_n x_1 \rightarrow$$
$$\rightarrow x_1 = x_2 = \cdots = x_n] \qquad \text{pour } n \geqslant 1.$$

On va voir inversement que dans toute réalisation $\mathfrak{M}$ qui satisfait l'ensemble des F_n, $\bar{P}$ peut être plongé dans un ordre total, ou encore que $\mathfrak{M}$ a une extension qui satisfait

$$\{ \mathscr{A}, \wedge x \wedge y[x \leqslant y \vee y \leqslant x] \} .$$

Il suffit pour cela de le montrer pour chaque sous-réalisation $\mathfrak{M}'$ de $\mathfrak{M}$ engendrée par un ensemble fini c'est-à-dire pour chaque sous-réalisation de $\mathfrak{M}$ dont l'ensemble de base est fini. Pour cela on opère par récurrence sur le nombre k d'éléments de E' ensemble de base de $\mathfrak{M}'$.

Soient $a_1, ..., a_k$ les éléments de E'. Il existe un i $(1 \leqslant i \leqslant k)$ tel que, pour tout $j \neq i$, $(a_i, a_j) \notin \overline{P}$: sinon on a une suite $n_1, n_2, ..., n_p, ...$ d'entiers compris entre 1 et k tels que

$$(a_1, a_{n_1}) \in \overline{P} ; (a_{n_1}, a_{n_2}) \in \overline{P} ; ... ; (a_{n_p}, a_{n_{p+1}}) \in \overline{P}, ... ;$$

ce qui contredit certainement une des F_n.

On peut supposer que a_k a cette propriété. Comme $E'' = (a_1, ..., a_{k-1})$ a $k - 1$ éléments, $\overline{P}$ se plonge dans un ordre total sur E'' (hypothèse de récurrence) ; il suffit de poser $a_k \geqslant a_1$; $a_k \geqslant a_2$; ... ; $a_k \geqslant a_{k-1}$ pour plonger $\overline{P}$ dans un ordre total sur E'.

Sur l'ensemble $\{ 1, 2, ..., n \}$ considérons la relation $\overline{P}$ dont les éléments sont $(1, 2), (2, 3), ..., (n - 1, n), (n, 1)$. Il est immédiat qu'on a ainsi un modèle de $(F_1, F_2, ..., F_{n-1}, \neg F_n)$ ce qui montre que l'ensemble des F_n n'équivaut à aucun de ses sous-ensembles finis, donc à aucun ensemble fini de conséquences d'après le théorème de finitude.

6. *a*) On considère le langage $\mathscr{L}_0$ constitué par un seul symbole fonctionnel à 2 variables : $\times$. Montrer qu'il existe un ensemble U de formules closes purement universelles de $\mathscr{L}_0$ telles que, pour qu'un groupe puisse être totalement ordonné, il faut et il suffit qu'il satisfasse U. Donner un tel ensemble dans le cas d'un groupe commutatif.

b) Même question pour un corps, le langage $\mathscr{L}_0$ étant constitué par : deux symboles fonctionnels : $+$, $\times$ à 2 variables ; un symbole de constante : 0.

Solution. — Conséquences faciles du théorème de plongement. Les ensembles cherchés sont, pour un groupe commutatif :

$$\bigwedge x \bigwedge y \, [x^n = y^n \rightarrow x = y]$$

pour $n \geqslant 1$ (groupe sans torsion) et pour un corps commutatif :

$$\bigwedge x_1 \dots \bigwedge x_n [x_1^2 + \cdots + x_n^2 = 0 \rightarrow x_1 = \cdots = x_n = 0]$$

pour $n \geqslant 1$ (corps réel).

7. Soit $\mathscr{L}$ un langage égalitaire contenant un symbole relationnel R à 2 variables, différent de $=$; montrer qu'il est impossible de trouver un ensemble $\mathscr{A}$ de formules de $\mathscr{L}$ ayant un modèle égalitaire infini, tel que dans tout modèle égalitaire de $\mathscr{A}$ la valeur de R soit un bon ordre sur l'ensemble de base.

Solution. — Soit $\mathscr{A}$ un ensemble de formules de $\mathscr{L}$, $\mathfrak{M}$ un modèle infini de $\mathscr{A}$ d'ensemble de base E, tel que la valeur $\overline{R}$ de R dans ce modèle soit un bon ordre sur E ; E contient donc une suite infinie strictement croissante $\xi_1, \xi_2, ..., \xi_n, ...$ Donc $(\xi_i, \xi_{i+1}) \in \overline{R}$ et $\xi_i \neq \xi_{i+1}$. Ajoutons

à $\mathscr{L}$ une suite infinie de symboles de constante $a_1, a_2, ..., a_n, ...$ Pour chaque entier n l'ensemble

$$(\mathscr{A} \; ; \; Ra_2\, a_1 \wedge a_2 \neq a_1 \; ; \; Ra_3\, a_2 \wedge a_3 \neq a_2 \; ; ... ; \; Ra_n\, a_{n-1} \wedge a_n \neq a_{n-1})$$

a un modèle : le modèle $\mathfrak{M}$, avec $\bar{a}_1 = \xi_n$; $\bar{a}_2 = \xi_{n-1}$; ... ; $\bar{a}_n = \xi_1$. Il en résulte (théorème de finitude) que l'ensemble

$$(\mathscr{A} \; ; \; Ra_1\, a_2 \wedge a_2 \neq a_1 \; ; ... ; \; Ra_n\, a_{n-1} \wedge a_n \neq a_{n-1} \; ; ...)$$

a un modèle. Dans ce modèle les valeurs de $a_1, ..., a_n, ...$ forment une suite infinie strictement décroissante, et par suite la valeur de R n'est pas un bon ordre.

8. (Existence de modèles libres). Soient $\mathscr{L}$ un langage égalitaire et $\mathscr{A}$ un ensemble de formules closes de $\mathscr{L}$ de la forme

$$\Lambda x_1 \ldots \Lambda x_n[(A_1 \wedge \cdots \wedge A_m) \rightarrow B]$$

(m pouvant être nul), où les A_i ($1 \leqslant i \leqslant m$) et B sont des formules atomiques.

a) Montrer que $\mathscr{A}$ est satisfait par la réalisation suivante de $\mathscr{L}$: son ensemble de base est le quotient de $T_{\mathscr{L}}$ (ensemble des termes de $\mathscr{L}$) par la relation d'équivalence $t \sim t' \Leftrightarrow t = t'$ est une conséquence de $\mathscr{A}$; la classe d'équivalence du terme t de $\mathscr{L}$ sera désignée par $[t]$. Pour chaque symbole fonctionnel f à n variables de $\mathscr{L}$, sa valeur $\bar{f}$ est définie par

$$\bar{f}([t_1], ..., [t_n]) = [ft_1 \ldots t_n] \, .$$

Pour chaque symbole relationnel R à n variables de $\mathscr{L}$, sa valeur $\bar{R}$ est définie par $([t_1], ..., [t_n]) \in \bar{R} \Leftrightarrow Rt_1 \ldots t_n$ est conséquence de $\mathscr{A}$.

b) En déduire que si $C_1, ..., C_p$ sont des formules atomiques et si

$$C_1 \vee \cdots \vee C_p$$

est conséquence de $\mathscr{A}$, l'une des C_i est conséquence de $\mathscr{A}$.

Solution. — *a*) Les axiomes de l'égalité pour le langage $\mathscr{L}$ ont aussi la forme $\Lambda x_1 \ldots \Lambda x_n[(A_1 \wedge \cdots \wedge A_m) \rightarrow B]$, avec $m = 1$ ou $m = 2$. Soient alors $t_1, ..., t_n$ des termes de $\mathscr{L}$; si $([t_1], ..., [t_n]) \in \bar{A}_i$ ($1 \leqslant i \leqslant m$), chaque formule $A_i(t_1, ..., t_n)$ est conséquence de $\mathscr{A}$, et donc aussi $B(t_1, ..., t_n)$; donc $([t_1], ..., [t_n]) \in \bar{B}$.

b) Chaque C_i a la forme $R_i(t_1, ..., t_{p_i})$ où R_i est un symbole relationnel de $\mathscr{L}$, et $t_1, ..., t_{p_i}$ des termes de $\mathscr{L}$. Puisque $C_1 \vee \cdots \vee C_p$ est conséquence de $\mathscr{A}$, elle est satisfaite dans la réalisation étudiée au *a*), et donc une des C_i est satisfaite par cette réalisation. Mais cela veut dire que cette formule C_i est conséquence de $\mathscr{A}$.

---

4. ÉLIMINATION DES QUANTIFICATEURS

Résumé

La théorie générale donnée dans les chapitres précédents va être appliquée à des systèmes axiomatiques possédant la propriété suivante : toute formule (appartenant au langage du système axiomatique considéré) est équivalente à une formule sans quantificateurs. Les exemples donnés dans le texte portent sur : certains groupes commutatifs discrètement (et totalement) ordonnés ; les corps algébriquement fermés ; les corps réels fermés; les anneaux booléens «séparables». Comme conséquences importantes de cette propriété, on obtient: 1° une caractérisation complète de toutes les relations qui sont explicitement définissables dans le système axiomatique considéré ; 2° (souvent) la saturation. Parmi les applications utiles du 2°, on a : dans le cas des corps algébriquement fermés, le « Nullstellensatz » de Hilbert (exercice 6); et, dans le cas des corps réels fermés, le théorème d'Artin sur la représentation des formes positives (exercice 4).

On indiquera (p. 48) une condition simple, portant sur les modèles, qui peut souvent être utilisée pour démontrer l'impossibilité d'une élimination des quantificateurs (exercices 1 et 2) même pour les systèmes axiomatiques saturés ; on trouvera une espèce de réciproque de cette condition dans le chapitre 6 (exercice 1). L'exercice 5 fournit une application algébrique, obtenue en combinant le 1° avec le théorème sur la définissabilité donné dans le précédent chapitre.

L'exercice 3 indique une méthode pour démontrer la saturation de certains systèmes axiomatiques sans utiliser l'élimination des quantificateurs (en faisant intervenir, à la place, certaines considérations de nature plus nettement algébrique). Pour l'emploi, dans ce genre de question, de la méthode plus générale des ultraproduits, cf. Kochen, *Annals of Math.* (2), **74** (1961) et Keisler [*Proc. Kon. Ned. Akad. Wet.*, **64**, 1961)], et ses applications aux corps *p*-adiques cf. Ax-Kochen [*Amer. J. Math.*, **87** (1965)] (On trouvera un traitement qui utilise la méthode de l'exercice 1, du chapitre 6 à la place des ultraproduits, dans leur article récent [*Annals of Math.* (2), **83** (1966)].)

Les résultats de ce chapitre ne sont utilisés dans la suite que dans quelques contre-exemples.

Tous les langages et toutes les réalisations étudiés dans ce chapitre sont supposés égalitaires.

On considère un langage $\mathscr{L}$ et un ensemble $\mathscr{A}$ de formules de $\mathscr{L}$. On dit que $\mathscr{A}$ permet l'élimination des quantificateurs dans une formule F de $\mathscr{L}$ s'il

existe une formule F' de $\mathscr{L}$ sans quantificateurs telle que $F \leftrightarrow F'$ soit conséquence de $\mathscr{A}$ (telle que dans tout modèle égalitaire de $\mathscr{A}$ on ait $\overline{F} = \overline{F'}$). On dit que $\mathscr{A}$ permet l'élimination des quantificateurs dans $\mathscr{L}$ s'il permet l'élimination des quantificateurs dans toute formule de $\mathscr{L}$.

Il est clair (par récurrence sur le nombre de quantificateurs de la formule F supposée prénexe) qu'il suffit pour cela que $\mathscr{A}$ permette l'élimination des quantificateurs dans toute formule de la forme $\bigvee xH$, où H est sans quantificateurs. D'après le théorème p. 7 du calcul propositionnel, chaque formule H sans quantificateurs équivaut à une formule de la forme $H_1 \vee \cdots \vee H_k$, où H_i est lui-même de la forme $\alpha_1 \wedge \cdots \wedge \alpha_r$, chaque α étant soit une formule atomique de $\mathscr{L}$, soit la négation d'une telle formule. Comme $\bigvee x[H_1 \vee \cdots \vee H_k]$ équivaut à $(\bigvee xH_1) \vee \cdots \vee (\bigvee xH_k)$ on a le théorème suivant :

THÉORÈME. — *Pour qu'un ensemble $\mathscr{A}$ permette l'élimination des quantificateurs dans $\mathscr{L}$, il faut et il suffit qu'il permette l'élimination des quantificateurs dans toute formule de $\mathscr{L}$ de la forme $\bigvee x[\alpha_1 \wedge \cdots \wedge \alpha_r]$ où chaque α_i est une formule atomique de $\mathscr{L}$ ou la négation d'une telle formule.*

Un ensemble $\mathscr{A}$ de formules est dit *saturé* dans $\mathscr{L}$, si pour toute formule close F de $\mathscr{L}$, F ou $\neg F$ est conséquence de $\mathscr{A}$.

THÉORÈME. — *Si $\mathscr{A}$ permet l'élimination des quantificateurs dans $\mathscr{L}$, et si $D_{\mathfrak{M}}$ est le diagramme d'un modèle $\mathfrak{M}$ de $\mathscr{A}$, $(\mathscr{A}, D_{\mathfrak{M}})$ est saturé (pour son langage $\mathscr{L}'$).*

Remarquons d'abord que si $\mathscr{A}$ permet l'élimination des quantificateurs dans $\mathscr{L}$, il la permet aussi dans tout langage $\mathscr{L}'$ obtenu en ajoutant à $\mathscr{L}$ un ensemble C de symboles de constantes. Car si F est une formule de $\mathscr{L}'$, soit F_1 la formule de $\mathscr{L}$ obtenue en substituant à chaque $a \in C$ qui apparaît dans F une variable x n'apparaissant pas dans F et distincte pour chaque a. On a une formule sans quantificateurs F_1' équivalente à F_1 et la substitution inverse donne une formule sans quantificateurs équivalente à F.

Soit alors F une formule close de $\mathscr{L}'$. Si elle est satisfaite dans le modèle $\mathfrak{M}$, on a $\overline{F} = E^{V_{\mathscr{L}}}$ (E étant l'ensemble de base de $\mathfrak{M}$). On sait que tout modèle de $D_{\mathfrak{M}}$ est une extension $\mathfrak{M}'$ de $\mathfrak{M}$. Considérons un modèle $\mathfrak{M}'$ de $(\mathscr{A}, D_{\mathfrak{M}})$. Dans $\mathfrak{M}$ et $\mathfrak{M}'$ qui sont des modèles de $\mathscr{A}$, F équivaut à une formule sans quantificateurs. D'après le lemme, (p. 37) si $\overline{\overline{F}}$ est la valeur de F dans $\mathfrak{M}'$ on a

$$\overline{F} = \overline{\overline{F}} \cap E^{V_{\mathscr{L}}} = E^{V_{\mathscr{L}}} .$$

Il en résulte que $\overline{\overline{F}}$ est non vide. F étant close, $\mathfrak{M}'$ satisfait donc F. Par suite F est conséquence de $(\mathscr{A}, D_{\mathfrak{M}})$ si elle est satisfaite par $\mathfrak{M}$. Comme pour toute formule F close, soit F, soit $\neg F$ est satisfaite par $\mathfrak{M}$ le théorème est démontré.

Le reste du chapitre est consacré à l'étude de quelques cas particuliers.

I. — Ordres denses avec premier et dernier élément.

On considère le langage $\mathscr{L}$ suivant : 2 symboles de constante 0, 1 ; 2 symboles relationnels à 2 variables : $<$; $=$.

On considère l'ensemble $\mathscr{A}$ des formules suivantes :

$\Lambda x \neg (x < x)$; $\Lambda x \Lambda y \Lambda z(x < y \wedge y < z \rightarrow x < z)$;

$\Lambda x \Lambda y(x = y \vee x < y \vee y < x)$ (axiomes de relation d'ordre total)

$\Lambda x \Lambda y \mathrm{V} z(x < y \rightarrow x < z \wedge z < y)$ (axiome de densité)

$\Lambda x(x = 0 \vee 0 < x)$; $\Lambda x(x = 1 \vee x < 1)$ (axiomes du 1[er] et du dernier élément).

On veut montrer que $\mathscr{A}$ permet l'élimination des quantificateurs dans $\mathscr{L}$. Pour cela on prend une formule de la forme $\mathrm{V}x[\alpha_1 \wedge \cdots \wedge \alpha_r]$ où chaque α est soit une formule atomique de $\mathscr{L}$, soit sa négation. On a donc pour α les possibilités : $t_1 < t_2$; $t_1 = t_2$; $\neg (t_1 < t_2)$; $t_1 \neq t_2$ (où t_1 et t_2 sont des termes de $\mathscr{L}$, ici 0, 1, ou une variable).

D'après $\mathscr{A}$, $\neg (t_1 < t_2)$ équivaut à $(t_2 < t_1) \vee t_1 = t_2$, et $t_1 \neq t_2$ équivaut à $t_1 < t_2 \vee t_2 < t_1$. En utilisant le fait que $A \wedge (B \vee C)$ équivaut à $(A \wedge B) \vee (A \wedge C)$ et que $\mathrm{V}x(A \vee B)$ équivaut à $(\mathrm{V}xA) \vee (\mathrm{V}xB)$ on est ramené à éliminer les quantificateurs dans une formule de la forme $\mathrm{V}x(\alpha_1 \wedge \cdots \wedge \alpha_r)$, où α est de la forme $t_1 < t_2$ et $t_1 = t_2$.

On opère par récurrence sur r. Pour $r = 1$ la formule est $\mathrm{V}x(t_1 < t_2)$ ou $\mathrm{V}x(t_1 = t_2)$, où t_1 et t_2 sont 0, 1 ou une variable. L'élimination est immédiate. Supposons l'élimination effectuée au rang $r - 1$ et considérons la formule $\mathrm{V}x(\alpha_1 \wedge \cdots \wedge \alpha_r)$. Remarquons que chaque α_i doit contenir x. Sinon, si par exemple α_1 ne le contient pas, la formule équivaut à $\alpha_1 \wedge \mathrm{V}x(\alpha_2 \wedge \cdots \wedge \alpha_r)$ et on est ramené au rang $r - 1$. Par suite la formule s'écrit

$$\mathrm{V}x(x < t_1 \wedge \cdots \wedge x < t_k \wedge u_1 < x \wedge \cdots \wedge u_l < x \wedge x = v_1 \wedge \cdots \wedge x = v_m) ,$$

où les t, u, v sont des termes qu'on peut supposer différents de x (si par exemple t_1 est x la formule équivaut à $\perp$; si v_1 est x on est ramené au rang $r - 1$).

Si $k > 1$, la formule équivaut à :

$$[t_1 < t_2 \wedge \mathrm{V}x(x < t_1 \wedge x < t_3 \wedge \cdots)] \vee [\neg (t_1 < t_2) \wedge \mathrm{V}x(x < t_2 \wedge x < t_3 \wedge \cdots)]$$

et on est ramené au rang $r - 1$.

De même si $l > 1$.

Si $k = l = 1$ la formule s'écrit

$$\mathrm{V}x(x < t_1 \wedge u_1 < x \wedge x = v_1 \wedge \cdots \wedge x = v_m)$$

qui, pour $m \neq 0$, équivaut à

$$(v_1 = v_2 = \cdots = v_m) \wedge (u_1 < v_1 < t_1)$$

et pour $m = 0$ à $u_1 < t_1$. Pour $k = 0$ la formule est

$$\vee x(u_1 < x \wedge x = v_1 \wedge \cdots \wedge x = v_m)$$

qui, pour $m = 0$, équivaut à $u_1 \neq 1$. De même pour $l = 0$ la formule équivaut à $t_1 \neq 0$. C. q. f. d.

Le lecteur pourra étudier de même les ordres denses avec premier mais sans dernier élément (supprimer la constante 1 et ajouter l'axiome $\wedge x \vee y(x < y)$) avec dernier mais sans premier élément, et sans premier ni dernier élément.

Remarquons que la formule sans quantificateurs équivalente à

$$\vee x(\alpha_1 \wedge \cdots \wedge \alpha_r)$$

contient les mêmes variables que cette formule sauf x. Il en résulte que pour toute formule close F la formule sans quantificateurs associée ne contient pas de variables. Les variables propositionnelles sont donc $0 < 1$, $0 = 1$ et $1 < 0$ qui sont respectivement équivalentes à $\top$, $\perp$ et $\perp$. Il en résulte que F est équivalente soit à $\top$ soit, à $\perp$, c'est-à-dire que *l'ensemble $\mathscr{A}$ ci-dessus est saturé pour son langage $\mathscr{L}$.*

II. — Ordre discret sans premier ni dernier élément.

Le langage $\mathscr{L}$ est constitué par : un symbole fonctionnel à une variable : s (lire « successeur ») ; un symbole relationnel à 2 variables : $<$ (sans compter $=$). Les termes de $\mathscr{L}$ sont donc de la forme $s^p x$ (s répété p fois, suivi d'une variable x).

On considère l'ensemble $\mathscr{A}$ des formules suivantes :

a) axiomes d'ordre total (voir ci-dessus) ;

b) $\wedge x \wedge y(x < y \leftrightarrow y = sx \vee sx < y)$; $\wedge x \vee y(x = sy)$.

Pour montrer que $\mathscr{A}$ permet d'éliminer les quantificateurs on se ramène comme ci-dessus à une formule de la forme $\vee x[\alpha_1 \wedge \cdots \wedge \alpha_r]$ où chaque α est de la forme $t_1 < t_2$ ou $t_1 = t_2$, c'est-à-dire $s^{p_1}x_1 < s^{p_2}x_2$ ou $s^{p_1}x_1 = s^{p_2}x_2$. On opère par récurrence sur r. Comme ci-dessus on voit immédiatement que x_1 ou x_2 doit être x. Si tous les deux sont x, un des α est du type $s^{p_1}x = s^{p_2}x$ ou $s^{p_1}x < s^{p_2}x$ et équivaut à $s^{p_1}x' = s^{p_2}x'$ ou à $s^{p_1}x' < s^{p_2}x'$, avec $x \neq x'$, ce qui ramène au rang $r - 1$.

Pour simplifier l'écriture, les formules $s^p x < x_1$ et $s^p x = x_1$ seront écrites $x < s^{-p} x_1$ et $x = s^{-p} x_1$. Les formules $s^p x < s^{p_1}x_1$ et $s^p x = s^{p_1}x_1$ sont alors toujours équivalentes à $x < s^{p_1 - p} x_1$ et à $x = s^{p - p_1} x_1$. La formule donnée s'écrit donc :

$$\vee x(x < t_1 \wedge \cdots \wedge x < t_k \wedge u_1 < x \wedge \cdots \wedge u_l < x \wedge x = v_1 \wedge \cdots \wedge x = v_m),$$

où les t, u, v sont de la forme $s^p y$ avec $p \in \mathbf{Z}$.

Si k ou l est > 1 on passe au rang $r - 1$ comme dans le cas précédent. On est donc ramené à

$$\bigvee x(x < t_1 \wedge u_1 < x \wedge x = v_1 \wedge \cdots \wedge x = v_m),$$

qui se traite de façon analogue au cas précédent. De même on montre que $\mathscr{A}$ *est saturé pour le langage* $\mathscr{L}$.

III. — Certains groupes commutatifs totalement ordonnés discrets.

Le langage $\mathscr{L}$ est le suivant : 2 symboles de constante : 0, 1 ; un symbole fonctionnel à 1 variable : $-$; un symbole fonctionnel à 2 variables : $+$; un symbole relationnel à 1 variable : > 0.

Les termes $1 + \cdots + 1$ et $t + \cdots + t$ (1 et t répétés p fois, où t est un terme) seront notés p et pt. Le terme $t + (- t')$ sera noté $t - t'$. On considère l'ensemble $\mathscr{A}$ des formules suivantes :

a) $\bigwedge x \bigwedge y \bigwedge z[(x + y) + z = x + (y + z)]$; $\bigwedge x \bigwedge y(x + y = y + x)$;
$\bigwedge x(x + 0 = x)$; $\bigwedge x(x - x = 0)$

(axiomes de groupe commutatif).

b) $\bigwedge x \bigwedge y(x > 0 \wedge y > 0 \rightarrow x + y > 0)$;
$\bigwedge x \neg (x > 0 \wedge - x > 0)$; $\bigwedge x(x = 0 \vee x > 0 \vee - x > 0)$

(ordre total compatible avec la loi du groupe).

c) $\bigwedge x(x > 0 \leftrightarrow x = 1 \vee x - 1 > 0)$ (ordre discret).

Il est immédiat (par récurrence sur la longueur de t) que pour tout terme t de $\mathscr{L}$ il existe des entiers $a_1, \ldots, a_n$, $b \in \mathbf{Z}$ et des variables $x_1, \ldots, x_n$ tels que $t = a_1 x_1 + \cdots + a_n x_n + b$ soit conséquence de $\mathscr{A}$ (en fait seulement des axiomes de groupe commutatif).

On peut montrer (voir exercice 2) que l'ensemble $\mathscr{A}$ des formules ci-dessus ne permet pas d'élimination des quantificateurs dans $\mathscr{L}$. Soit $\mathscr{L}'$ le langage obtenu en ajoutant à $\mathscr{L}'$ pour chaque entier $n > 1$ le symbole relationnel à 1 variable : $n \mid$ (lire « n divise... ») et soit $\mathscr{A}'$ l'ensemble des formules obtenues en ajoutant à $\mathscr{A}$ les formules suivantes :

d) $\bigwedge x[n \mid x \leftrightarrow \bigvee y(x = ny)]$ (pour chaque $n > 1$),

e) $\bigwedge x[n \mid x \vee n \mid x + 1 \vee \cdots \vee n \mid x + n - 1]$ (pour chaque $n > 1$).

Il est clair que tout modèle de $\mathscr{A}$ (c'est-à-dire tout groupe commutatif ordonné discret) est aussi un modèle de *d*) (plus exactement, on peut pour chaque modèle de $\mathscr{A}$ choisir la valeur de $n \mid$ d'une façon et d'une seule de façon à satisfaire *d*)). Par contre *e*) n'est pas conséquence de (*a*, *b*, *c*, *d*). On peut montrer (exercice 2) que (*a*, *b*, *c*, *d*) ne permet pas l'élimination des quantificateurs dans $\mathscr{L}'$. On va voir par contre que (*a*, *b*, *c*, *d*, *e*) $= \mathscr{A}'$ la permet.

On considère pour cela une formule F de $\mathscr{L}'$ de la forme $\bigvee x(\alpha_1 \wedge \cdots \wedge \alpha_n)$, où α_i est une formule atomique de $\mathscr{L}'$ ou sa négation, donc est de l'une des formes suivantes : $t_1 = t_2$ (qui équivaut, d'après $\mathscr{A}$, à $t = 0$ avec $t = t_1 - t_2$) ; $t \neq 0$; $t > 0$; $\neg(t > 0)$; $n \mid t$; $\neg(n \mid t)$.

Remarquons que $t \neq 0$ équivaut (d'après $\mathscr{A}'$) à $t > 0 \vee -t > 0$, que $\neg(t > 0)$ équivaut à $t = 0 \vee -t > 0$ et que $\neg(n \mid t)$ équivaut à

$$n \mid t + 1 \vee \cdots \vee n \mid t + n - 1 \quad \text{(d'après } e\text{)}.$$

Il en résulte qu'on peut supposer α_i de l'une des formes suivantes :

$$t = 0,\ t > 0,\ n \mid t.$$

Ecrivons chaque terme t sous la forme $px + t'$ avec $p \in \mathbf{Z}$, t' étant un terme qui ne contient pas la variable x. Pour plus de clarté la formule $t_1 - t_2 > 0$ sera aussi écrite $t_1 > t_2$.

La formule F prend alors la forme :

$$\bigvee x(p_1 x > t_1 \wedge \cdots \wedge p_k x > t_k \wedge q_1 x = u_1 \wedge \cdots \wedge q_l x = u_l \wedge \\ \wedge n_1 \mid r_1 x - v_1 \wedge \cdots \wedge n_m \mid r_m x - v_m)$$

où les $p, q, r \in \mathbf{Z}$ et les t, u, v sont des termes ne contenant pas x. Remarquons que d'après $\mathscr{A}$ la formule $n_1 \mid r_1 x - v_1$ équivaut à :

$$(n_1 \mid r_1 x \wedge n_1 \mid v_1) \vee (n_1 \mid r_1 x + 1 \wedge n_1 \mid v_1 + 1) \vee \cdots \vee \\ \vee (n_1 \mid r_1 x + n_1 - 1 \wedge n_1 \mid v_1 + n_1 - 1)\ .$$

En faisant cette substitution dans F (et en utilisant le fait que $A \wedge (B \vee C)$ équivaut à $(A \wedge B) \vee (A \wedge C)$) on est ramené à étudier une formule de la même forme que F mais où $v_1, \ldots, v_m$ sont des entiers (positifs, négatifs, ou nuls).

Posons

$$h = |p_1| + \cdots + |p_k| + |q_1| + \cdots + |q_l| \\ + n_1 + \cdots + n_m + |r_1| + \cdots + |r_m|\ .$$

On va opérer par récurrence sur h, que nous appellerons le rang de F. On suppose donc l'élimination effectuée pour toutes les formules de rang $\leqslant h - 1$. Si $k \geqslant 2$, F équivaut à :

$$[p_2 t_1 \geqslant p_1 t_2 \wedge \bigvee x(p_1 x > t_1 \wedge p_3 x > t_3 \wedge \cdots)] \vee \\ \vee [p_1 t_2 > p_2 t_1 \wedge \bigvee x(p_2 x > t_2 \wedge p_3 x > t_3 \wedge \cdots)]$$

et on est ramené à 2 formules de rang $\leqslant h - 1$.

Si $l \geqslant 2$ remarquons que $q_1 x = u_1 \wedge q_2 x = u_2$ équivaut à

$$q_1 x = u_1 \wedge (q_2 - q_1) x = u_2 - u_1\ .$$

En supposant $| q_1 | \leqslant | q_2 |$, on a

$$| q_1 | + | q_1 - q_2 | < | q_1 | + | q_2 | .$$

Par suite cette substitution ramène à une formule de rang $\leqslant h - 1$.

Si $k = 1$ et $l = 1$ la formule F s'écrit :

$$\mathsf{V}x(px > t \wedge qx = u \wedge n_1 \mid r_1 x - v_1 \wedge \cdots \wedge n_m \mid r_m x - v_m) .$$

Elle équivaut à

$$pu > qt \wedge q \mid u \wedge qn_1 \mid r_1 u - v_1 q \wedge \cdots \wedge qn_m \mid r_m u - v_m q ,$$

qui est sans quantificateur.

Si $k = 0$ et $l = 1$ on a la même formule sans quantificateur, en supprimant $pu > qt \wedge$.

Supposons alors $k = 1$ et $l = 0$ (le cas où $k = 0$ et $l = 0$ se traitant de même). F s'écrit

$$\mathsf{V}x(px > t \wedge n_1 \mid r_1 x - v_1 \wedge \cdots \wedge n_m \mid r_m x - v_m) .$$

Si l'un des n_i par exemple n_1 s'écrit $n_1 = nn'$, n et n' étant premiers entre eux, $n_1 \mid r_1 x - v_1$ équivaut à

$$n \mid r_1 x - v_1 \wedge n' \mid r_1 x - v_1 .$$

Comme $n + n' < n_1$ on est ramené au rang $h - 1$. Il en résulte qu'on peut supposer tous les n_i de la forme $p_i^{\rho_i}$ où p_i est premier.

Soient alors $a_1, ..., a_k$ les entiers de l'intervalle $[0, n_1 - 1]$ qui sont tels que $n_1 \mid r_1 a_1 - v_1, ..., n_1 \mid r_1 a_k - v_1$ (s'il en existe). La formule $n_1 \mid r_1 x - v_1$ équivaut (comme on le vérifie facilement) à :

$$n_1 \mid x - a_1 \vee \cdots \vee n_1 \mid x - a_k .$$

En effectuant cette substitution dans F on est ramené à k formules de rang $h - 1$.

Il en résulte qu'on peut supposer $r_1 = r_2 = \cdots = r_m = 1$ et F s'écrit :

$$\mathsf{V}x(px > t \wedge n_1 \mid x - v_1 \wedge \cdots \wedge n_m \mid x - v_m) .$$

Si $n_1 = p^{\rho_1}$, $n_2 = p^{\rho_2}$ avec $\rho_1 \leqslant \rho_2$ par exemple, $n_1 \mid x - v_1 \wedge n_2 \mid x - v_2$ équivaut à $n_1 \mid v_1 - v_2 \wedge n_2 \mid x - v_2$. On peut donc supposer les n_i de la forme $p_i^{\rho_i}$, les p_i étant des nombres premiers distincts ; $n_1, ..., n_m$ étant premiers entre eux deux à deux, on sait qu'il existe un entier u et un seul de l'intervalle $[0, n_1 n_2 ... n_m - 1]$ tel que

$$n_1 \mid u - v_1 ; ... ; n_m \mid u - v_m .$$

Il en résulte que F est équivalente à $\top$: en effet en supposant par exemple $p \geqslant 0$, pour $t \geqslant 0$, $x = u + n_1 \dots n_m t$ satisfait

$$px > t \wedge n_1 \mid x - v_1 \wedge \cdots \wedge n_m \mid x - v_m ,$$

et pour $t < 0$, $x = u$ la satisfait aussi. C. q. f. d.

Comme ci-dessus on voit que si F est une formule close, la formule F' sans quantificateurs qui lui est équivalente n'a pas de variables libres. Les formules atomiques sont donc $t = 0$; $t > 0$; $n \mid t$, où t est un terme de $\mathscr{L}'$ sans variables, c'est-à-dire un entier de $\mathbf{Z}$. Par suite chacune de ces formules atomiques équivaut à $\top$ ou à $\perp$, donc aussi F' et par suite aussi F, ce qui montre que $\mathscr{A}'$ *est saturé pour* $\mathscr{L}'$.

IV. — Corps algébriquement clos.

Le langage $\mathscr{L}$ est le suivant : 2 symboles de constante : 0, 1 ; un symbole fonctionnel à 1 variable : $-$; 2 symboles fonctionnels à 2 variables : $+$ et $\times$. Aucun symbole relationnel (sauf $=$). L'ensemble $\mathscr{A}$ est formé des formules suivantes :

a) $\bigwedge x \bigwedge y \bigwedge z[(x + y) + z = x + (y + z)]$; $\bigwedge x \bigwedge y(x + y = y + x)$;
$\bigwedge x(x + 0 = x)$; $\bigwedge x[x + (-x) = 0]$
(axiomes de groupe commutatif pour $+$).

b) $\bigwedge x \bigwedge y \bigwedge z[(xy)z = x(yz)]$; $\bigwedge x \bigwedge y(xy = yx)$; $\bigwedge x(x.1 = x)$;
$\bigwedge x \bigvee y(x = 0 \vee xy = 1)$; $\bigwedge x \bigwedge y \bigwedge z[x(y + z) = xy + xz]$; $0 \neq 1$.

Il est clair que tout modèle de *a*), *b*) est un corps commutatif et que pour tout terme t de $\mathscr{L}$ il existe un polynôme $p(x_1, \dots, x_n)$ à coefficients dans $\mathbf{Z}$ tel que $t = p(x_1, \dots, x_n)$ soit conséquence de *a*), *b*). (Le terme $1 + 1 + \cdots + 1$ (1 répété p fois) étant noté p, et le terme $t \times \cdots \times t$ (t répété p fois) étant noté t^p).

c) Pour chaque $n > 1$ la formule :

$$\bigwedge x_0 \bigwedge x_1 \dots \bigwedge x_{n-1} \bigvee x(x_0 + x_1 x + x_2 x^2 + \cdots + x_{n-1} x^{n-1} + x^n = 0).$$

Il est clair que les modèles de $\mathscr{A} = (a, b, c)$ sont les corps algébriquement clos. On va voir que $\mathscr{A}$ permet l'élimination des quantificateurs dans $\mathscr{L}$.

LEMME. — *Soient* $p(x_1, \dots, x_k, x)$ *et* $q(x_1, \dots, x_k, x)$ *deux termes de* $\mathscr{L}$ *(c'est-à-dire deux polynômes à coefficients dans* $\mathbf{Z}$*). Alors il existe une formule* F *de* $\mathscr{L}$*, sans quantificateurs, telle que dans tout modèle de* (a, b) *(corps commutatif* K*)* $\bar{F}$ *soit l'ensemble des* $(\xi_1, \dots, \xi_k) \in K^k$ *tels que* $p(\xi_1, \dots, \xi_k, x)$ *divise* $q(\xi_1, \dots, \xi_k, x)$.

Posons

$$p(x) = a_0 + a_1 x + \cdots + a_m x^m \quad \text{et} \quad q(x) = b_0 + b_1 x + \cdots + b_n x^n ,$$

où les a_i et b_i sont des polynômes en $x_1, \dots, x_k$ à coefficients dans $\mathbf{Z}$. On opère

par récurrence sur $m + n$. Il est clair que pour $m + n = 0$ la formule F cherchée est $a_0 \neq 0 \vee b_0 = 0$.

Si $n < m$, par hypothèse il y a une formule F correspondant au couple de polynômes $p_1 = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}$ et $q(x)$. La formule cherchée est alors

$$(a_m \neq 0 \wedge b_0 = b_1 = \cdots = b_n = 0) \vee (a_m = 0 \wedge F).$$

Pour $n \geqslant m$ posons

$$p_1 = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} ; \quad q_1 = a_m q(x) - b_n x^{n-m} p(x)$$

(q_1 est de degré $< n$). Par hypothèse il existe une formule F correspondant au couple p_1, q et une formule G correspondant au couple p, q_1. Alors la formule cherchée est :

$$(a_m = 0 \wedge F) \vee (a_m \neq 0 \wedge G). \qquad \text{C. q. f. d.}$$

Considérons alors une formule F de $\mathscr{L}$ de la forme

$$\mathsf{V}x(\alpha_1 \wedge \cdots \wedge \alpha_r),$$

où chaque α est une formule atomique de $\mathscr{L}$ ou sa négation, donc est de la forme $t_1 = t_2$ ou $t_1 \neq t_2$. Chaque α équivaut donc à une formule de la forme $t = 0$ ou $t \neq 0$ (où $t = t_1 - t_2$). D'autre part comme

$$t_1 \neq 0 \wedge t_2 \neq 0 \wedge \cdots \wedge t_l \neq 0$$

équivaut à $t_1 t_2 \ldots t_l \neq 0$ on voit que la formule F s'écrit

$$\mathsf{V}x(t_1 = 0 \wedge t_2 = 0 \wedge \cdots \wedge t_k = 0 \wedge t \neq 0).$$

Chaque t_i est un polynôme en x (dont les coefficients sont des polynômes en d'autres variables à coefficients dans $\mathbf{Z}$) dont nous écrirons le terme de plus haut degré $a_i x^{n_i}$. Il est clair qu'on peut supposer chaque $n_i \neq 0$: si par exemple $n_1 = 0$, F équivaut à

$$t_1 = 0 \wedge \mathsf{V}x(t_2 = 0 \wedge \cdots \wedge t_k = 0 \wedge t \neq 0).$$

On opère par récurrence sur la somme des n_i. Si $k \geqslant 2$, supposons par exemple $n_1 \geqslant n_2$ et posons

$$t_1' = a_2 t_1 - a_1 x^{n_1 - n_2} t_2 \qquad \text{et} \qquad t_2' = t_2 - a_2 x^{n_2} ;$$

t_1' est donc de degré $< n_1$ et t_2' de degré $< n_2$. La formule F équivaut à :

$$[a_2 = 0 \wedge \mathsf{V}x(t_1 = 0 \wedge t_2' = 0 \wedge \cdots \wedge t_k = 0 \wedge t \neq 0)] \vee$$
$$\vee [a_2 \neq 0 \wedge \mathsf{V}x(t_1' = 0 \wedge t_2 = 0 \wedge \cdots \wedge t_k = 0 \wedge t \neq 0)]$$

et on est ramené à 2 formules de rang inférieur (le rang d'une formule étant ici la somme des n_i).

Si $k = 1$ la formule F s'écrit $\vee x(t_1 = 0 \wedge t \neq 0)$. On sait que dans tout corps algébriquement clos K, étant donnés deux polynômes $p(x)$ et $q(x)$ à coefficients dans K à 1 variable, pour qu'il existe un x tel que $p(x) = 0$ et $q(x) \neq 0$ il faut et il suffit que p ne divise pas q^n pour n assez grand, par exemple n = degré de p. Par suite si G est la formule sans quantificateur associée d'après le lemme au couple t_1, t^n (n étant le degré en x du polynôme t_1), la formule F équivaut à $\neg G$ (c'est-à-dire a la même valeur que $\neg G$ dans tout corps algébriquement clos).

Si $k = 0$ la formule F s'écrit $\vee x(t \neq 0)$. Posons $t = a_0 + a_1 x + \cdots + a_n x^n$. Comme tout corps algébriquement clos est infini, et que tout polynôme à une variable n'a qu'un nombre fini de racines sauf s'il est $\equiv 0$, on voit que F équivaut à

$$a_0 \neq 0 \vee a_1 \neq 0 \vee \cdots \vee a_n \neq 0 . \qquad \text{C. q. f. d.}$$

On voit comme ci-dessus que toute formule close de $\mathscr{L}$ équivaut à une formule sans quantificateurs dont les formules atomiques sont de la forme $t = 0$ (où t ne contient pas de variables), donc $n = 0$ avec $n \in \mathbf{N}$. Or $n = 0$ ou $n \neq 0$ n'est pas conséquence de $\mathscr{A}$ pour $n > 1$ (car il existe des corps algébriquement clos de caractéristique p, pour $p = 0$ ou p premier). Il en résulte que $\mathscr{A}$ *n'est pas saturé* mais qu'il le devient si on lui ajoute *une* des formules $p = 0$ pour p premier (corps algébriquement clos de caractéristique p) ou l'ensemble des formules $p \neq 0$ pour p premier (corps algébriquement clos de caractéristique nulle).

Application : Théorème. — *Si les polynômes $p_1, \ldots, p_k$ en les variables $x_1, \ldots, x_n$ à coefficients dans un corps K ont un zéro commun dans une extension L de K ils ont un zéro commun algébrique sur K.*

En effet soit Ω la clôture algébrique de K, D_Ω le diagramme de Ω. Les axiomes $\mathscr{A}$ de corps algébriquement clos permettant l'élimination des quantificateurs, $(\mathscr{A}, D_\Omega)$ est saturé (th. p. 48). Soit $\mathscr{L}'$ le langage de $(\mathscr{A}, D_\Omega)$. La formule

$$\vee x_1 \ldots \vee x_n(p_1 = 0 \wedge \cdots \wedge p_k = 0)$$

est une formule de $\mathscr{L}'$ qui est satisfaite dans un modèle de $(\mathscr{A}, D_\Omega)$: la clôture algébrique de L. Il en résulte qu'elle est satisfaite dans tous les modèles de $(\mathscr{A}, D_\Omega)$ et en particulier dans Ω.

V. — Corps réels fermés.

Le langage $\mathscr{L}$ considéré est formé de : deux symboles de constante : 0, 1 ; 1 symbole fonctionnel à 1 variable : $-$; 2 symboles fonctionnels à 2 variables : $+$, $\times$; un symbole relationnel à 1 variable : > 0. L'ensemble $\mathscr{A}$ est formé de :

a) les axiomes de corps commutatif : (voir au § IV formules *a*) et *b*))

b) $\bigwedge x \bigwedge y(x > 0 \wedge y > 0 \rightarrow x + y > 0)$; $\bigwedge x(x = 0 \vee x > 0 \vee -x > 0)$;

$\bigwedge x \neg (x > 0 \wedge -x > 0)$; $\bigwedge x \bigwedge y(x > 0 \wedge y > 0 \rightarrow xy > 0)$.

Tout modèle des axiomes *a*) et *b*) est un corps ordonné.

c) $\bigwedge x \bigvee y(x = y^2 \vee -x = y^2)$;

$\bigwedge x_0 \bigwedge x_1 \dots \bigwedge x_{2n} \bigvee x(x_0 + x_1 x + \cdots + x_{2n} x^{2n} + x^{2n+1} = 0)$ pour chaque $n \geqslant 1$.

Il est clair que les modèles de $\mathscr{A} = (a, b, c)$ sont les corps réels fermés ; (pour les propriétés des corps réels fermés utilisées dans la suite voir par exemple : van der Waerden, *Modern Algebra*). On va montrer que $\mathscr{A}$ permet l'élimination des quantificateurs dans $\mathscr{L}$.

Pour tout terme t, il existe comme dans le cas précédent un polynôme $p(x_1, \dots, x_n)$ à coefficients dans $\mathbf{Z}$ tel que $t = p(x_1, \dots, x_n)$ soit conséquence de $\mathscr{A}$.

Pour simplifier l'écriture, la formule $t - t' > 0$ sera aussi écrite $t > t'$ ou $t' < t$ et la formule $t < t' \wedge t' < t''$ sera écrite $t < t' < t''$. Toute formule atomique de $\mathscr{L}$, soit F, est équivalente à une formule de la forme

$$p(x, x_1, \dots, x_n) = 0 \qquad \text{ou} \qquad p(x, x_1, \dots, x_n) > 0 \,.$$

Par définition le degré en x de F est le degré en x du polynôme p. Pour toute formule F sans quantificateurs, le degré en x de F est par définition le maximum des degrés en x des formules atomiques de F.

LEMME. — *Pour toute formule A sans quantificateurs de la forme :*

$$p_1 = 0 \wedge \cdots \wedge p_k = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0$$

(les p_i et q_i étant des polynômes en $x, x_1, \dots, x_n$) il existe une formule B sans quantificateurs équivalente à A (dans tout modèle de $\mathscr{A}$) dont le degré en x est $\leqslant$ au plus petit degré en x des polynômes p_i (chaque p_i étant supposé de degré non nul).

Par récurrence sur la somme des degrés en x des p_i, q_j. Supposons le lemme démontré quand cette somme est $\leqslant h - 1$ et soit

$$p_1 = 0 \wedge \cdots \wedge p_k = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0 \,,$$

une formule telle que la somme des degrés des p_i, q_j soit h.

Si $k \geqslant 2$, soient $a_1 x^{m_1}$ et $a_2 x^{m_2}$ les termes de plus haut degré de p_1 et p_2, et posons

$$\pi_1 = a_2 p_1 - a_1 x^{m_1 - m_2} p_2 \text{ (en supposant } m_1 \geqslant m_2) \text{ et } \pi_2 = p_2 - a_2 x^{m_2} \,.$$

Alors la formule considérée équivaut à

$$(a_2 = 0 \wedge p_1 = 0 \wedge \pi_2 = 0 \wedge \cdots \wedge p_k = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0) \vee$$
$$\vee (a_2 \neq 0 \wedge \pi_1 = 0 \wedge p_2 = 0 \wedge \cdots \wedge p_k = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0) .$$

On se ramène ainsi à 2 formules de rang $h - 1$.

Si $k = 0$ il n'y a rien à montrer. Pour $k = 1$ la formule s'écrit :

$$p = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0 .$$

Si tous les q_r sont de degré en x inférieur à celui de p la formule satisfait au lemme. Sinon q_1 par exemple est de degré supérieur à celui de p. Soient ax^m et bx^n les termes de plus haut degré de p et q_1 (avec $n \geqslant m$). Posons

$$P = p - ax^m,\ Q = a^2 q_1 - abx^{n-m} p.$$

Alors la formule équivaut à :

$$(a = 0 \wedge P = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0) \vee$$
$$\vee (a \neq 0 \wedge p = 0 \wedge Q > 0 \wedge q_2 > 0 \wedge \cdots \wedge q_l > 0)$$

et on est ramené à 2 formules de rang $\leqslant h - 1$.

Théorème. — *Soit $A(x, x_1, \ldots, x_n)$ une formule sans quantificateurs de degré h en x. Soient a, b deux variables (distinctes de $x, x_1, \ldots, x_n$). Alors, il existe une formule sans quantificateurs B dont les variables sont $a, b, x_1, \ldots, x_n$, dont le degré en a (ou b) est $\leqslant h$, dont chaque formule atomique contient soit a, soit b, soit ni a ni b (mais pas les 2 ensemble), et telle que*

$B \leftrightarrow \mathsf{V}x[a < x < b \wedge A(x, x_1, \ldots, x_n)]$ *soit conséquence de* $(\mathscr{A}, a < b)$.

Par récurrence sur le degré en x de A. Si ce degré est nul, A ne contient pas x. Par suite la formule $\mathsf{V}x(a < x < b \wedge A)$ équivaut à $A \wedge a < b$. La formule cherchée est A.

A est équivalente à une disjonction de formules de la forme $u_1 \wedge \cdots \wedge u_r$ où chaque u est une formule atomique ou sa négation, donc est de l'une des formes : $p = 0$; $p \neq 0$; $p > 0$; $\neg (p > 0)$. Comme $p \neq 0$ équivaut à

$$p > 0 \vee -p > 0 , \quad \text{et} \quad \neg(p > 0) \text{ à } p = 0 \vee -p > 0$$

on voit qu'on peut supposer A de la forme

$$p_1 = 0 \wedge \cdots \wedge p_k = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0.$$

Le lemme montre alors que si $k \geqslant 2$, ou si $k = 1$ avec un des q_i de degré en x supérieur ou égal au degré de p_1, on est ramené à une formule de degré inférieur et on applique l'hypothèse de récurrence. Il en résulte qu'on peut supposer A de la forme I :

$$p = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0 \quad (\text{avec } d^\circ q_i < d^\circ p = h = d^\circ A)$$

ou de la forme II :

$$q_1 > 0 \wedge \cdots \wedge q_l > 0 .$$

Supposons d'abord A de la forme II. On considère donc la formule :

$$F = \vee x(a < x < b \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0) .$$

Or dans tout corps réel fermé, pour que les polynômes $q_1, \ldots, q_l, q_{l+1} = x - a$, $q_{l+2} = b - x$ soient simultanément positifs, il faut et il suffit qu'il existe un intervalle $]\,\alpha, \beta\,[$ (où α, β sont racines de l'un des q_i) dans lequel ils sont simultanément positifs. Si dans cet intervalle une des différences

$$q_i - q_j \; (1 \leqslant i < j \leqslant l + 2)$$

s'annule, la formule

$$\vee x(a < x < b \wedge q_i - q_j = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0) = F_{ij}$$

est satisfaite. Si aucune des différences $q_i - q_j$ ne s'annule dans $]\alpha, \beta[$ chacune reste de signe constant dans $]\alpha, \beta[$ et on a par exemple dans cet intervalle $0 < q_1 < q_2 < \cdots < q_{l+2}$. Par suite α, β sont toutes deux racines de q_1 et il y a un point de $]\alpha, \beta[$ qui annule q_1' (dérivée de q_1 par rapport à x). Alors la formule :

$$F_i = \vee x(a < x < b \wedge q_1' = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0)$$

est satisfaite. Il en résulte que dans tout modèle de $(\mathscr{A}, a < b)$ la formule F entraîne

$$\left(\bigvee_{i,j} F_{ij}\right) \vee \left(\bigvee_i F_i\right).$$

Comme cette dernière entraîne évidemment F (chaque F_{ij} et chaque F_i entraînent F) les deux formules sont équivalentes. Or chacune des F_{ij} ou F_i est de degré $\leqslant h$ et de la forme I. Il en résulte qu'on peut maintenant supposer A de la forme I, c'est-à-dire de la forme

$$p = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0 , \quad \text{avec} \quad d^\circ q_i < d^\circ p = h = d^\circ A .$$

La formule suivante est évidemment équivalente à A :

$$\begin{aligned}(p = 0 \wedge p' = 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0) \\ \vee (p = 0 \wedge p' > 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0) \vee \\ \vee (p = 0 \wedge - p' > 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0) = A_1 \vee A_2 \vee A_3 .\end{aligned}$$

La formule $\vee x(a < x < b \wedge A_1)$ se traite immédiatement en appliquant le lemme (car $d^\circ p'$ en $x \leqslant h - 1$) puis l'hypothèse de récurrence. On considère donc la formule :

$$\vee x(a < x < b \wedge p = 0 \wedge p' > 0 \wedge q_1 > 0 \wedge \cdots \wedge q_l > 0) .$$

Dans un corps réel fermé, cette formule est satisfaite si et seulement si p a une racine simple, comprise entre a et b, qui rende positifs tous les polynômes p', $q_1, \ldots, q_l$ (pour des valeurs fixées, données à a, b, $x_1, \ldots, x_n$). Pour cela il faut et il suffit qu'il existe un intervalle $]\alpha, \beta[$ avec $a \leqslant \alpha < \beta \leqslant b$ où α, β sont racines de p', ou $q_1 \ldots$ ou q_l dans lequel $p', q_1, \ldots, q_l$ sont positifs et tels que $p(\alpha) < 0$ et $p(\beta) > 0$.

Considérons deux nouvelles variables u, v. D'après l'hypothèse de récurrence la formule :

$$\bigwedge z[u < z < v \rightarrow p'(z) > 0 \wedge q_1(z) > 0 \wedge \cdots \wedge q_l(z) > 0]$$

qui peut s'écrire

$$\neg \bigvee z[u < z < v \wedge (-p'(z) \geqslant 0 \vee -q_1(z) \geqslant 0 \vee \cdots \vee -q_l(z) \geqslant 0)]$$

équivaut à une formule $Q(u, v)$ sans quantificateurs, dont le degré en u et v est $\leqslant h - 1$ et dans laquelle aucune formule atomique ne contient à la fois u et v. La formule considérée équivaut donc à la disjonction des formules suivantes :

$$\bigvee u \bigvee v[a \leqslant u < v \leqslant b \wedge p(u) < 0 \wedge p(v) > 0 \wedge q_i(u) = 0 \wedge \\ \wedge q_j(v) = 0 \wedge Q(u, v)]$$

pour $1 \leqslant i \leqslant j \leqslant l + 1$ en posant $p' = q_{l+1}$.

Considérons par exemple la formule obtenue en prenant $i = 1, j = 2$:

$$\bigvee u \bigvee v[a \leqslant u < v \leqslant b \wedge p(u) < 0 \wedge p(v) > 0 \wedge q_1(u) = 0 \wedge \\ \wedge q_2(v) = 0 \wedge Q(u, v)].$$

On l'écrit comme disjonction des formules suivantes :

a) $\bigvee u \bigvee v[a < u < v < b \wedge p(u) < 0 \wedge p(v) > 0 \wedge q_1(u) = 0 \wedge \wedge q_2(v) = 0 \wedge Q(u, v)]$

b) $p(b) > 0 \wedge q_2(b) = 0 \wedge \bigvee u[a < u < b \wedge p(u) < 0 \wedge q_1(u) = 0 \wedge \wedge Q(u, b)]$

c) $p(a) < 0 \wedge q_1(a) = 0 \wedge \bigvee v[a < v < b \wedge p(v) > 0 \wedge q_2(v) = 0 \wedge \wedge Q(a, v)]$

d) $p(a) < 0 \wedge p(b) > 0 \wedge q_1(a) = 0 \wedge q_2(b) = 0 \wedge Q(a, b)$

(qui est sans quantificateurs et de la forme exigée dans l'énoncé).

Nous traiterons seulement le cas *a*), les cas *b*) et *c*) s'en déduisant facilement. Appliquons le lemme aux deux formules

$$p(u) < 0 \wedge q_1(u) = 0 \qquad \text{et} \qquad p(v) > 0 \wedge q_2(v) = 0 ,$$

ce qui donne deux formules $H_1(u)$, $H_2(v)$ de degrés $\leqslant h - 1$. La formule devient :

$$\bigvee u \bigvee v[a < u < v < b \wedge H_1(u) \wedge H_2(v) \wedge Q(u, v)] .$$

Ecrivons la formule

$$H_1(u) \wedge H_2(v) \wedge Q(u, v)$$

sous la forme d'une disjonction de formules de la forme $K_1 \wedge \cdots \wedge K_r$ où chaque K est une formule atomique apparaissant dans la formule précédente ou sa négation. Par suite chaque K contient soit u soit v mais pas les deux, et est de degré $\leqslant h - 1$. La formule considérée s'écrit donc comme disjonction des formules suivantes :

$$\bigvee u \bigvee v[a < u < v < b \wedge K_1(u) \wedge \cdots \wedge K_{r'}(u) \wedge K_{r'+1}(v) \wedge \cdots \wedge K_r(v)] .$$

D'après l'hypothèse de récurrence la formule :

$$\bigvee v[u < v < b \wedge K_{r'+1}(v) \wedge \cdots \wedge K_r(v)]$$

équivaut (mod. $\mathscr{A}$, $u < b$) à une formule $M(u, b)$ sans quantificateurs, de degré en u et $b \leqslant h - 1$ et dans laquelle chaque formule atomique ne contient pas à la fois u et b. On peut donc écrire $M(u, b)$ comme disjonction de formules de la forme :

$$M_1(u) \wedge \cdots \wedge M_{s'}(u) \wedge M_{s'+1}(b) \wedge \cdots \wedge M_s(b) .$$

La formule considérée s'écrit alors comme disjonction de formules de la forme :

$$\bigvee u[a < u < b \wedge K_1(u) \wedge \cdots \wedge K_{r'}(u) \wedge M_1(u) \wedge \cdots \wedge M_{s'}(u)] \wedge$$
$$\wedge M_{s'+1}(b) \wedge \cdots \wedge M_s(b)$$

auxquelles il suffit d'appliquer l'hypothèse de récurrence. C. q. f. d.

THÉORÈME. — *$\mathscr{A}$ permet l'élimination des quantificateurs dans $\mathscr{L}$.*

Il suffit de le montrer pour une formule de la forme $\bigvee x A(x, x_1, ..., x_n)$. Ajoutons à $\mathscr{L}$ deux constantes u et $\frac{1}{u}$ et à $\mathscr{A}$ l'axiome $u \cdot \frac{1}{u} = 1$. Le théorème précédent montre que la formule :

$$\bigvee x \left[- 1 < x < 1 \wedge A\left(\frac{x}{u}, x_1, ..., x_n\right)\right]$$

équivaut à une formule sans quantificateur Q. Chaque formule atomique de Q est de la forme $p\left(\frac{1}{u}\right) = 0$ ou $p\left(\frac{1}{u}\right) > 0$. D'après l'axiome $u \cdot \frac{1}{u} = 1$ elle équivaut

à une formule de la forme $p(x, u) = 0$ ou $p(x, u) > 0$. Donc il existe une formule sans quantificateur $R(z)$ (où z est une variable de $\mathscr{L}$) telle que

$$\vee x\left[-1 < x < 1 \wedge A\left(\frac{x}{u}, x_1, \dots, x_n\right)\right]$$

soit équivalente à $R(u)$ (mod. $\mathscr{A}$, $u \cdot \frac{1}{u} = 1$). Il est clair que dans tout modèle de $\mathscr{A}$, les deux formules

$$\vee x A(x, x_1, \dots, x_n) \quad \text{et} \quad \vee z[0 < x < 1 \wedge R(z)]$$

sont équivalentes. Or d'après le théorème précédent cette dernière formule équivaut à une formule sans quantificateurs. C. q. f. d.

En particulier il en résulte que $\mathscr{A}$ *est saturé* : en effet les formules atomiques sans variable de $\mathscr{L}$ sont de la forme $n = 0$ (avec $n \in \mathbf{Z}$) ou $n > 0$. La première équivaut à $\perp$ sauf si $n = 0$ (car tout corps réel fermé est de caractéristique nulle) et la seconde à $\top$ ou à $\perp$.

VI. — Anneaux de Boole séparables.

Le langage $\mathscr{L}$ considéré est formé de deux symboles de constante : 0, 1, deux symboles fonctionnels à 2 variables : $+$ et $\times$. L'ensemble $\mathscr{A}$ est formé de :

a) $\wedge x \wedge y \wedge z[(x + y) + z = x + (y + z)]$, $\wedge x \wedge y(x + y = y + x)$; $\wedge x(x + 0 = x)$, $\wedge x \vee y(x + y = 0)$ (axiomes de groupe commutatif pour $+$).

b) $\wedge x \wedge y \wedge z[(xy) z = x(yz)]$; $\wedge x[x \cdot 1 = 1 \cdot x = x]$; $\wedge x \wedge y \wedge z[x(y + z) = xy + xz]$; $1 \neq 0$.

c) $\wedge x[x^2 = x]$.

a) et *b*) forment les axiomes de la structure d'anneau avec unité ; *a*), *b*) et *c*) ceux de la structure d'anneau de Boole.

Tout anneau de Boole est commutatif et satisfait $\wedge x(2x = 0)$: en effet on a

$$(x + 1)^2 = x + 1 = x^2 + 2x + 1, \text{ donc } 2x = 0 ;$$

d'autre part $(x + y)^2 = x + y$, d'où $xy + yx = 0$ et par suite $xy = yx$.

Si x, y sont des termes de $\mathscr{L}$, le terme $x + y + xy$ sera écrit $x \cup y$; la formule $xy = y$ sera écrite aussi $y \subset x$. Il est clair que les termes de $\mathscr{L}$ sont les polynômes $p(x_1, \dots, x_n)$ du premier degré en chacune des variables $x_1, \dots, x_n$ et à coefficients 0 ou 1.

Désignons par $F(x)$ la formule :

$$x \neq 0 \wedge \wedge y[y \subset x \rightarrow y = 0 \vee y = x] .$$

Les éléments qui satisfont cette formule sont appelés *atomes*.

Ajoutons au langage $\mathscr{L}$ une suite infinie de symboles relationnels à 1 variable que nous désignerons par $B, A_1, A_2, \ldots, A_n, \ldots$, et à l'ensemble $\mathscr{A}$ les formules suivantes :

$$d) \quad \bigwedge x\left[A_n x \leftrightarrow \bigvee x_1 \ldots \bigvee x_n\left[\bigwedge_{1\leqslant i<j\leqslant n} x_i \neq x_j \bigwedge_{i=1}^{n} (F(x_i) \wedge x_i \subset x)\right]\right]$$

pour $n = 1, 2, \ldots$

$$\bigwedge x[Bx \leftrightarrow \bigwedge y[y \subset x \wedge y \neq 0 \rightarrow A_1 y]] .$$

Il est clair que dans tout modèle de *a*), *b*), *c*) on peut définir d'une façon et d'une seule les valeurs de $B, A_1, A_2, \ldots$ de façon à satisfaire les formules *d*). Les éléments qui satisfont $A_n x$ sont ceux qui contiennent n atomes distincts. Les éléments qui satisfont Bx sont dits atomiques (tout sous-ensemble contient un atome). Un anneau de Boole sera dit *séparable*, s'il satisfait l'axiome

e) $\bigvee x[Bx \wedge \neg A_1(1 + x)]$, c'est-à-dire si on peut séparer l'unité en deux parties disjointes dont l'une est atomique et l'autre sans atome.

Nous allons montrer que les formules *a*), *b*), *c*), *d*), *e*) permettent l'élimination des quantificateurs pour leur langage $\mathscr{L}'$.

Remarquons que chaque terme de $\mathscr{L}'$ contenant x est de la forme $ax + b$ où a et b sont des termes ne contenant pas x. Les formules atomiques de $\mathscr{L}'$ sont donc $ax = b$, $B(ax + b)$, $A_n(ax + b)$, où a et b sont des termes ne contenant pas x.

LEMME 1. — *Soit $\Phi(x)$ une formule sans quantificateur de $\mathscr{L}'$. Alors la formule $\bigvee x[F(x) \wedge \Phi(x)]$ équivaut à une formule sans quantificateur.*

— On peut supposer que $\Phi(x)$ est conjonction de formules atomiques et de négations de formules atomiques.

1) $\Phi(x)$ est de la forme

$$a_1 x = 0 \wedge a_2 x = 0 \wedge \cdots \wedge a_k x = 0 \wedge x \neq b_1 \wedge \cdots \wedge x \neq b_l .$$

On montre le lemme par récurrence sur la longueur de $\Phi(x)$; $\Phi(x)$ équivaut à

$$ax = 0 \wedge x \neq b_1 \wedge \cdots \wedge x \neq b_l , \qquad \text{où} \qquad a = a_1 \cup a_2 \cup \cdots \cup a_k .$$

Donc $\bigvee x[F(x) \wedge \Phi(x)]$ équivaut à la disjonction des formules suivantes :

a) $\bigvee x[F(x) \wedge ax = 0 \wedge x \neq b_1 \wedge \cdots \wedge x \neq b_l] \wedge ab_i \neq 0 \, (i = 1, 2, \ldots, l)$,

qui équivaut à

$$\bigvee x[F(x) \wedge ax = 0 \wedge x \neq b_1 \wedge \cdots \wedge x \neq b_{i-1} \wedge x \neq b_{i+1} \wedge \cdots \wedge x \neq b_l] \wedge ab_i \neq 0,$$

c'est-à-dire à

$$\vee x[F(x) \wedge \Psi(x)] \wedge ab_i \neq 0\,,$$

$\Psi(x)$ étant plus courte que $\Phi(x)$. On peut donc appliquer l'hypothèse de récurrence.

b) $\vee x[F(x) \wedge ax = 0 \wedge x \neq b_1 \wedge \cdots \wedge x \neq b_l] \wedge (b_i = b_j)\,(1 \leqslant i < j \leqslant l)$,

qui équivaut à

$$\vee x[F(x) \wedge ax = 0 \wedge x \neq b_1 \wedge \cdots \wedge x \neq b_{i-1} \wedge x \neq b_{i+1} \wedge \cdots \wedge x \neq b_l] \wedge (b_i = b_j)\,,$$

à laquelle on applique l'hypothèse de récurrence.

c) $\vee x[F(x) \wedge ax = 0 \wedge x \neq b_1 \wedge \cdots \wedge x \neq b_l] \wedge \neg F(b_i)\,(i = 1, 2, ..., l)$,

qui équivaut à

$$\vee x[F(x) \wedge ax = 0 \wedge x \neq b_1 \wedge \cdots \wedge x \neq b_{i-1} \wedge x \neq b_{i+1} \wedge \cdots \wedge x \neq b_l] \wedge \neg F(b_i)\,,$$

à laquelle on applique l'hypothèse de récurrence.

d) $\vee x[F(x) \wedge ax = 0 \wedge x \neq b_1 \wedge \cdots \wedge x \neq b_l] \wedge$

$$\wedge \bigwedge_{i=1}^{l} F(b_i) \bigwedge_{i=1}^{l} (ab_i = 0) \bigwedge_{1 \leqslant i < j \leqslant l} (b_i \neq b_j)$$

qui équivaut à

$$A_{l+1}(1 + a) \bigwedge_{i=1}^{l} F(b_i) \bigwedge_{i=1}^{l} (ab_i = 0) \bigwedge_{1 \leqslant i < j \leqslant l} (b_i \neq b_j).$$

2) Dans le cas général on écrit $\Phi(x) = \Phi_1(x) \wedge \Phi_2(x)$, où $\Phi_1(x)$ est de la forme précédente. On montre le lemme par récurrence sur la longueur de $\Phi_2(x)$. Si celle-ci est nulle on est ramené au cas précédent.

— Si $\Phi_2(x) = \Psi(x) \wedge ax = b$, alors $\vee x[F(x) \wedge ax = b \wedge \Psi(x) \wedge \Phi_1(x)]$ équivaut à

$$\{\vee x[F(x) \wedge \Psi(x) \wedge ax = 0 \wedge \Phi_1(x)] \wedge (b = 0)\} \vee \{F(b) \wedge \Psi(b) \wedge \Phi_1(b) \wedge ab = b\}$$

à laquelle on peut appliquer l'hypothèse de récurrence puisque $\Psi(x)$ est plus courte que $\Phi_2(x)$.

— Si $\Phi_2(x) = \Psi(x) \wedge ax \neq b$, alors $\mathsf{V}x[F(x) \wedge ax \neq b \wedge \Psi(x) \wedge \Phi_1(x)]$ équivaut à

$$\{ \mathsf{V}x[F(x) \wedge \Psi(x) \wedge ax = 0 \wedge \Phi_1(x)] \wedge b \neq 0 \} \vee$$
$$\vee \{ \mathsf{V}x[F(x) \wedge \Psi(x) \wedge ax = x \wedge x \neq b \wedge \Phi_1(x)] \} .$$

On peut appliquer l'hypothèse de récurrence aux deux parties de cette disjonction puisque $ax = x$ peut s'écrire $(1 + a)\, x = 0$.

— Si $\Phi_2(x) = \Psi(x) \wedge (\neg)\, A_n(ax + b)$ (c'est-à-dire si $\Phi_2(x)$ est de l'une des deux formes $\Psi(x) \wedge A_n(ax + b)$ ou $\Psi(x) \wedge \neg A_n(ax + b)$) alors

$$\mathsf{V}x[F(x) \wedge (\neg)\, A_n(ax + b) \wedge \Psi(x) \wedge \Phi_1(x)]$$

équivaut à

$$\{ \mathsf{V}x[F(x) \wedge \Psi(x) \wedge ax = 0 \wedge \Phi_1(x)] \wedge (\neg)\, A_n\, b \}$$
$$\vee \{\mathsf{V}x[F(x) \wedge \Psi(x) \wedge ax = x \wedge x \subset b \wedge \Phi_1(x)] \wedge (\neg)\, A_{n+1}\, b \} \vee$$
$$\vee \{ \mathsf{V}x[F(x) \wedge \Psi(x) \wedge ax = x \wedge bx = 0 \wedge \Phi_1(x)] \wedge (\neg)\, A_{n-1}\, b \} .$$

On peut appliquer l'hypothèse de récurrence aux trois parties de cette disjonction. En effet $ax = x$ s'écrit $x(1 + a) = 0$ et $x \subset b$ s'écrit $(1 + b)\, x = 0$.

— Si $\Phi_2\,(x) = \Psi(x) \wedge (\neg)\, B(ax + b)$, alors

$$\mathsf{V}x[F(x) \wedge (\neg)\, B(ax + b) \wedge \Psi(x) \wedge \Phi_1\,(x)]$$

équivaut à

$$\mathsf{V}x[F(x) \wedge \Psi(x) \wedge \Phi_1\,(x)] \wedge (\neg)\, Bb\, ,$$

à laquelle on peut appliquer l'hypothèse de récurrence.

LEMME 2. — *Soient $a_1, \ldots, a_n$, n termes de $\mathscr{L}$ ne contenant pas x. Il existe N termes $\alpha_1, \ldots, \alpha_N$ ne contenant pas x et $I_1, \ldots, I_n$, sous-ensembles de $\{ 1, 2, \ldots, N \}$ tels que*

$$\mathscr{A} \vdash \alpha_i\, \alpha_j = 0 \;\; (1 \leqslant i < j \leqslant N)\, ; \qquad \mathscr{A} \vdash a_r = \sum_{i \in I_r} \alpha_i \;\; (r = 1, \ldots, n)\, .$$

Démonstration par récurrence sur n. — Si $\beta_1, \beta_2, \ldots, \beta_K$ satisfont au lemme pour les termes $a_2, \ldots, a_n$, alors $a_1\, \beta_1, a_1\, \beta_2, \ldots, a_1\, \beta_K, (1 + a_1)\, \beta_1, \ldots, (1 + a_1)\, \beta_K$, $a_1 + a_1\, \beta_1 + \cdots + a_1\, \beta_K$, satisfont au lemme pour les termes $a_1, \ldots, a_n$.

LEMME 3. — *Soit $\Phi(x) = R_1(a_1\, x + b_1) \wedge \cdots \wedge R_n(a_n\, x + b_n)$, où $R_i(z)$ est l'une des formules suivantes :*

$$\neg A_1\, z\, ;\; Bz\, ;\; \neg Bz\, ;\; z = 0\, ;\; z \neq 0\, .$$

Alors $\Phi(x)$ équivaut à une disjonction de formules du même type où on a pour

tout i $(1 \leqslant i \leqslant n)$ *soit* $a_i = 0$, *soit* $a_i = b_i$, *soit* $b_i = 0$, *et pour tout couple* i, j $(1 \leqslant i < j \leqslant n)$ *soit* $a_i = a_j$, *soit* $\mathscr{A} \vdash a_i\, a_j = 0$.

Remarquons que si $R(z)$ est une des formules $\neg A_1\, z, Bz, \neg Bz, z = 0, z \neq 0$ et si $\mathscr{A} \vdash uv = 0$, alors $\mathscr{A} \vdash R(u + v) \leftrightarrow Ru \overset{\wedge}{\vee} Rv$ (c'est-à-dire $Ru \wedge Rv$ ou $Ru \vee Rv$).

Soient alors $\alpha_1, ..., \alpha_N$ les termes correspondant à $(a_1, a_2, ..., a_n, b_1, ..., b_n)$ d'après le lemme 2. On a pour $1 \leqslant r \leqslant n$:

$$a_r\, x + b_r = \Big(\sum_{i \in I_r} \alpha_i\Big) x + \sum_{i \in J_r} \alpha_i$$

où I_r et J_r sont des sous-ensembles de $\{ 1, 2, ..., N \}$.

Donc $$a_r\, x + b_r = \sum_{i \in I_r \cap J_r} \alpha_i\, x + \alpha_i + \sum_{i \in I_r - J_r} \alpha_i\, x + \sum_{i \in J_r - I_r} \alpha_i\,.$$

Donc $R_r(a_r\, x + b_r)$ équivaut soit à

$$\bigwedge_{i \in I_r \cap J_r} R_r(\alpha_i\, x + \alpha_i) \bigwedge_{i \in I_r - J_r} R_r(\alpha_i\, x) \bigwedge_{i \in J_r - I_r} R_r(\alpha_i)\,,$$

soit à

$$\bigvee_{i \in I_r \cap J_r} R_r(\alpha_i\, x + \alpha_i) \bigvee_{i \in I_r - J_r} R_r(\alpha_i\, x) \bigvee_{i \in J_r - I_r} R_r(\alpha_i)\,.$$

En substituant ces formules à chacun des $R_r(a_r\, x + b_r)$ dans $\Phi(x)$ et en utilisant la distributivité de $\wedge$ par rapport à $\vee$ on obtient le résultat cherché.

LEMME 4. — $\mathsf{V}x[R_1(a_1\, x + b_1) \wedge \cdots \wedge R_n(a_n\, x + b_n)]$ *équivaut à une formule sans quantificateurs.*

D'après le lemme 3 on peut supposer que pour $i \neq j$ on a soit $a_i = a_j$ soit $a_i\, a_j = 0$, et de plus $b_i = a_i$ ou $b_i = 0$. La formule considérée s'écrit donc

$$G = \mathsf{V}x[\Phi_1(a_1\, x) \wedge \cdots \wedge \Phi_k(a_k\, x)]\,, \quad \text{avec} \quad a_i\, a_j = 0 \quad \text{pour} \quad i \neq j\,.$$

Soit H la formule $\mathsf{V}x\Phi_1(a_1\, x) \wedge \cdots \wedge \mathsf{V}x\Phi_k(a_k\, x)$. Il est clair que H est conséquence de G. Mais d'autre part $\mathscr{A} \vdash H \to G$. En effet si H est satisfaite dans un modèle de $\mathscr{A}$ il existe des éléments $\xi_1, ..., \xi_k$ du modèle satisfaisant respectivement les formules $\Phi_1(a_1\, x), ..., \Phi_k(a_k\, x)$. Alors l'élément

$$a_1\, \xi_1 + \cdots + a_k\, \xi_k$$

satisfait simultanément ces formules (puisque $a_i\, a_j = 0$ pour $i \neq j$), ce qui montre que G est satisfaite.

Donc $\mathscr{A} \vdash G \leftrightarrow H$. D'après la forme de H on est ramené à étudier la formule $\mathsf{V}x\Phi_1(a_1\, x)$ qui est de la forme

$$\mathsf{V}x[R_1(ax) \wedge \cdots \wedge R_k(ax) \wedge R'_1(ax + a) \wedge \cdots \wedge R'_l(ax + a)]\,,$$

où $R_i(z)$ et $R'_j(z)$ sont l'une des formules

$$\neg A_1 z\,,\ Bz\,,\ \neg Bz\,,\ z = 0\,,\ z \neq 0\,.$$

On a donc $k \leqslant 3$, $l \leqslant 3$ (en éliminant les cas où parmi les R_i apparaîtrait une formule atomique et sa négation, la formule étant alors équivalente à $\bot$). On peut supposer que l'un des R_i est B ou $\neg B$: en effet

$$R_1(ax) \wedge \cdots \wedge R_3(ax) \wedge R'_1(ax + a) \wedge \cdots \wedge R'_3(ax + a)$$

équivaut à

$$[B(ax) \wedge R_1(ax) \wedge \cdots \wedge R'_3(ax + a)] \vee$$
$$\vee [\neg B(ax) \wedge R_1(ax) \wedge \cdots \wedge R'_3(ax + a)]\,.$$

De même on peut supposer que $ax = 0$ ou $ax \neq 0$ apparaissent, ainsi que

$$(\neg)\, B(ax + a)\,, (\neg)\, (ax + a = 0).$$

Si la formule $ax = 0$ ou $ax + a = 0$ apparaît l'élimination est immédiate : si par exemple $R_1(ax)$ est $ax = 0$ la formule équivaut à

$$R_2\, 0 \wedge R_3\, 0 \wedge R'_1\, a \wedge R'_2\, a \wedge R'_3\, a\,.$$

On peut donc supposer que $R'_1(ax)$ est $ax \neq 0$ et que $R'_1(ax + a)$ est $ax + a \neq 0$. Distinguons quatre cas :

a) $R_2(ax) = \neg A_1(ax)$ et $R'_2(ax + a) = \neg A_1(ax + a)$. La formule équivaut alors soit à $\bot$, soit à

$$\mathsf{V}x[ax \neq 0 \wedge \neg A_1(ax) \wedge ax + a \neq 0 \wedge \neg A_1(ax + a)]\,,$$

c'est-à-dire à $\neg A_1\, a \wedge a \neq 0$.

b) $R_2(ax) = \neg A_1(ax)$ et $\neg A_1(ax + a)$ n'apparaît pas. La formule équivaut alors à $\bot$ ou à l'une des formules suivantes :

$$\mathsf{V}x[ax \neq 0 \wedge \neg A_1(ax) \wedge ax + a \neq 0 \wedge B(ax + a)],$$
c'est-à-dire à $A_1\, a \wedge \neg Ba$;

(en effet, par hypothèse, on peut séparer l'unité, et donc aussi tout élément a, en deux parties disjointes dont l'une est atomique et l'autre sans atome).

$$\mathsf{V}x[ax \neq 0 \wedge \neg A_1(ax) \wedge ax + a \neq 0 \wedge \neg B(ax + a)],$$
c'est-à-dire $\neg Ba$.

c) $R'_2(ax + a) = \neg A_1(ax + a)$ et $\neg A_1(ax)$ n'apparaît pas : cas identique au précédent à l'échange près des R_i et R'_i.

d) $\neg A_1(ax)$ et $\neg A_1(ax + a)$ n'apparaissent pas. La formule considérée

équivaut alors à $\perp$ ou à l'une des formules suivantes (à l'échange près des R_i et des R'_i) :

$\mathsf{V}x[ax \neq 0 \wedge B(ax) \wedge ax + a \neq 0 \wedge B(ax + a)]$,
c'est-à-dire à $A_2\, a \wedge Ba$;

$\mathsf{V}x[ax \neq 0 \wedge B(ax) \wedge ax + a \neq 0 \wedge \neg B(ax + a)]$,
c'est-à-dire à $A_1\, a \wedge \dot{\neg} Ba$.

$\mathsf{V}x[ax \neq 0 \wedge \neg B(ax) \wedge ax + a \neq 0 \wedge \neg B(ax + a)]$,
c'est-à-dire à $\neg Ba$.

THÉORÈME. — *Si $\Phi(x)$ est sans quantificateurs, $\mathsf{V}x\Phi(x)$ équivaut à une formule sans quantificateurs.*

On peut supposer que $\Phi(x)$ est une conjonction de formules atomiques et de négations de formules atomiques. Elle s'écrit alors $\Phi_1(x) \wedge \Phi_2(x)$, où

$$\Phi_1(x) = R_1(a_1 x + b_1) \wedge \cdots \wedge R_n(a_n x + b_n),$$

les R_i étant de la forme décrite dans l'énoncé du lemme 3. On montre le théorème par récurrence sur la longueur de $\Phi_2(x)$. Si cette longueur est nulle on est ramené au lemme 4. Si $\Phi_2(x) = A_n(ax + b) \wedge \Psi(x)$, supposons d'abord $n = 1$. La formule à étudier est alors

$$\mathsf{V}x[A_1(ax + b) \wedge \Psi(x) \wedge \Phi_1(x)],$$

qui équivaut à

$$\mathsf{V}y\, \mathsf{V}x[F(y) \wedge y \subset ax + b \wedge \Psi(x) \wedge \Phi_1(x)].$$

D'après l'hypothèse de récurrence

$$\mathsf{V}x[\Psi(x) \wedge y \subset ax + b \wedge \Phi_1(x)]$$

équivaut à une formule sans quantificateur $H(y)$ (car $y \subset ax + b$ s'écrit $ayx + by + y = 0$). La formule considérée équivaut donc à $\mathsf{V}y[F(y) \wedge H(y)]$ donc à une formule sans quantificateur d'après le lemme 1.

Supposons montré que, pour tout $p < n$, tout couple de termes a, b ne contenant pas x et toute formule $\Phi_1(x)$ de la forme

$$R_1(a_1 x + b_1) \wedge \cdots \wedge R_j(a_j x + b_j),$$

la formule

$$\mathsf{V}x[A_p(ax + b) \wedge \Psi(x) \wedge \Phi_1(x)]$$

est équivalente à une formule sans quantificateurs. Alors la formule

$$\mathsf{V}x[A_n(ax + b) \wedge \Psi(x) \wedge \Phi_1(x)]$$

équivaut à

$$\mathsf{V}y\, \mathsf{V}x[F(y) \wedge y \subset ax + b \wedge A_{n-1}(ax + b + y) \wedge \Psi(x) \wedge \Phi_1(x)].$$

D'après l'hypothèse faite, la formule

$$\bigvee x[A_{n-1}(ax + b + y) \wedge y \subset ax + b \wedge \Psi(x) \wedge \Phi_1(x)]$$

équivaut à une formule sans quantificateur $H(y)$. La formule considérée équivaut donc à $\bigvee y[F(y) \wedge H(y)]$ donc à une formule sans quantificateur d'après le lemme 1.

Si $\Phi_2(x) = \neg A_n(ax + b) \wedge \Psi(x)$ (avec $n > 1$) la formule considérée est :

$$\bigvee x[\neg A_n(ax + b) \wedge \Psi(x) \wedge \Phi_1(x)] .$$

Elle équivaut à la disjonction des formules suivantes :

$$\bigvee x[\neg A_1(ax + b) \wedge \Psi(x) \wedge \Phi_1(x)]$$

à laquelle on peut appliquer l'hypothèse de récurrence ;

$$\bigvee x[A_i(ax + b) \wedge \neg A_{i+1}(ax + b) \wedge \Psi(x) \wedge \Phi_1(x)]$$

pour $i = 1, 2, ..., n - 1$. On traite cette formule par récurrence sur i. Elle équivaut à :

$$\bigvee y \bigvee x[F(y) \wedge y \subset ax + b \wedge A_{i-1}(ax + b + y) \wedge \neg A_i(ax + b + y) \wedge \Phi_1(x) \wedge \Psi(x)] .$$

D'après l'hypothèse de récurrence,

$$\bigvee x[y \subset ax + b \wedge A_{i-1}(ax + b + y) \wedge \neg A_i(ax + b + y) \wedge \Phi_1(x) \wedge \Psi(x)]$$

équivaut à une formule sans quantificateur $H(y)$. La formule considérée équivaut donc à $\bigvee y[F(y) \wedge H(y)]$ donc à une formule sans quantificateur d'après le lemme 1. C. q. f. d.

EXERCICES

1. Montrer que l'utilisation du symbole s est nécessaire pour l'élimination des quantificateurs dans la théorie des ordres discrets sans premier ni dernier élément. Plus précisément, si on considère le langage $\mathscr{L}$ constitué par le seul symbole $<$ (et $=$), et l'ensemble $\mathscr{A}$ des formules suivantes :

a) axiomes d'ordre total,

b) $\bigwedge x \bigvee y \bigwedge z(z > x \leftrightarrow z = y \vee z > y)$;

$$\bigwedge x \bigvee y \bigwedge z[z < x \leftrightarrow z = y \vee z < y],$$

les modèles de cet ensemble sont les mêmes que ceux du § II (ensembles totalement ordonnés discrets sans premier ni dernier élément), mais $\mathscr{A}$ ne permet pas l'élimination des quantificateurs dans $\mathscr{L}$.

Solution. — On considère le modèle de $\mathscr{A}$ constitué par l'ensemble ordonné **Z**. Si $D_{\mathbf{Z}}$ est le diagramme de ce modèle, et si $\mathscr{A}$ permet l'élimination des quantificateurs $(\mathscr{A}, D_{\mathbf{Z}})$ est saturé. Considérons le modèle constitué en ajoutant l'élément $\frac{1}{2}$ au modèle précédent. C'est une extension du modèle précédent donc elle satisfait $D_{\mathbf{Z}}$, ainsi que $\mathscr{A}$. Or la formule $\bigvee x[0 < x < 1]$ n'est pas satisfaite dans le premier modèle, et elle l'est dans le second ce qui contredit la saturation de $(\mathscr{A}, D_{\mathbf{Z}})$.

2. On considère le langage $\mathscr{L}$ utilisé au paragraphe III, mais sans les symboles $n \mid$ et l'ensemble des formules *a*), *b*), *c*) de ce paragraphe.

a) Montrer que cet ensemble ne permet pas l'élimination des quantificateurs.

b) On ajoute maintenant à $\mathscr{L}$ les symboles $n \mid$, et on considère l'ensemble des formules *a*), *b*), *c*), *d*). Montrer que cet ensemble ne permet pas l'élimination des quantificateurs dans $\mathscr{L}$.

Solution. — On considère le groupe $\mathbf{Z} \times \mathbf{Z} = G$ ordonné de la façon suivante : $(a, b) > 0$ si et seulement si $a > 0$ ou $a = 0$ et $b > 0$. G est un modèle de *a*), *b*), *c*), qui contient **Z** comme sous-modèle (en identifiant $(0, n)$ avec n). Soit $D_{\mathbf{Z}}$ le diagramme de **Z**. Alors $(a, b, c, d, D_{\mathbf{Z}})$ n'est pas saturé puisque la formule $\bigwedge x \bigvee y[x = 2y \vee x + 1 = 2y]$ est vraie dans **Z** mais non dans G.

3. *a*) Soit $\mathscr{A}$ un ensemble dénombrable de formules d'un langage égalitaire. Montrer que si $\mathscr{A}$ a un modèle (égalitaire) infini, pour chaque cardinal infini $\aleph$, $\mathscr{A}$ a un modèle de cardinal $\aleph$.

b) Montrer que si $\mathscr{A}$ n'a que des modèles infinis et s'il existe un cardinal infini $\aleph$ tel que tous les modèles de $\mathscr{A}$ de cardinal $\aleph$ soient isomorphes (c'est-à-dire si $\mathscr{A}$ est catégorique pour la classe des réalisations égalitaires de cardinal $\aleph$) alors $\mathscr{A}$ est saturé.

c) Montrer que tous les modèles dénombrables des axiomes du paragraphe I (ordre dense avec premier et dernier élément) sont isomorphes au segment $[0, 1]$ de l'ensemble des nombres dyadiques (rationnels dont le dénominateur est une puissance de 2). En déduire que les axiomes du paragraphe I sont saturés.

d) Nous utiliserons ici les propriétés des bases de transcendance des extensions d'un corps K (voir Bourbaki, *Algèbre*, Ch. V).

Montrer que si Ω est un corps algébriquement clos, si K et K' sont deux extensions algébriquement closes de Ω ayant des bases de transcendance équipotentes, K et K' sont isomorphes.

En déduire que deux corps algébriquement clos de même caractéristique, de puissance $2^{\aleph_0}$ sont isomorphes, et que les axiomes de corps algébriquement clos de caractéristique p ($p = 0$ ou p premier) sont saturés.

Solution. — *a*) Ajoutons à $\mathscr{L}$ un ensemble C de symboles de constantes de cardinal $\aleph$ et soit $\mathscr{B}$ l'ensemble des formules $a \neq b$ pour a, b éléments distincts de C. Tout sous-ensemble fini de $(\mathscr{A}, \mathscr{B})$ a un modèle (le modèle infini donné de $\mathscr{A}$). Donc l'ensemble tout entier a un modèle. Si $\hat{\mathscr{A}}$ est l'ensemble de $\hat{F}$ pour $F \in \mathscr{A}$ (formés avec des symboles fonctionnels tous distincts), $(\hat{\mathscr{A}}, \mathscr{B})$ a donc un modèle canonique dont le cardinal est évidemment $\aleph$.

b) Soit F une formule close de $\mathscr{L}$ non conséquence de $\mathscr{A}$. $(\mathscr{A}, \neg F)$ a donc un modèle, et par suite a un modèle de cardinal $\aleph$ ($\mathscr{A}$ n'ayant par hypothèse que des modèles infinis $(\mathscr{A}, \neg F)$ a un modèle infini). Comme tous les modèles de $\mathscr{A}$ de cardinal $\aleph$ sont isomorphes, $\neg F$ est satisfaite dans tous les modèles de $\mathscr{A}$ de cardinal $\aleph$. Par suite $\neg F$ est conséquence de $\mathscr{A}$: si $(\mathscr{A}, F)$ avait un modèle il aurait un modèle de cardinal $\aleph$. Il en résulte que $\mathscr{A}$ est saturé.

c) Il est clair que tout ensemble muni d'un ordre dense est infini. Soit alors $(0, a_1, ..., a_n, ...) \cup \{ 1 \}$ un ensemble dénombrable muni d'un ordre dense, dont le premier élément est 0 et le dernier 1. On définit par récurrence sur n une application φ de $\{ 0, a_1, ..., a_n, 1 \}$ dans le segment $[0, 1]$ des dyadiques, conservant l'ordre : si a_{n+1} se place entre a_i et a_j on pose

$$\varphi(a_{n+1}) = \tfrac{1}{2}[\varphi(a_i) + \varphi(a_j)] .$$

Tout nombre dyadique $\dfrac{2\,q + 1}{2^n}$ est atteint, sinon en supposant que $\dfrac{2\,r + 1}{2^n}$ est le premier dyadique qui n'est jamais atteint (le premier dans l'ordre : $\dfrac{2\,q + 1}{2^n} < \dfrac{2\,q' + 1}{2^{n'}}$ si $n < n'$ ou si $n = n'$ et $q < q'$) alors $\dfrac{r}{2^{n-1}}$ et $\dfrac{r + 1}{2^{n-1}}$ sont atteints et égaux à $\varphi(a_i)$ et $\varphi(a_j)$. Alors $\dfrac{2\,r + 1}{2^n} = \varphi(a_k)$, où a_k est le premier a qui se place entre a_i et a_j. Il en résulte que φ est un isomorphisme. C. q. f. d.

d) Soient b_i ($i \in I$) et b'_i ($i \in I$) des bases de transcendance de K et K' sur Ω ; K est donc algébrique sur $\Omega(b_i)_{i \in I}$; c'est donc la clôture algébrique de $\Omega(b_i)_{i \in I}$. De même K' est la clôture algébrique de $\Omega(b'_i)_{i \in I}$. Or $\Omega(b_i)_{i \in I}$ et $\Omega(b'_i)_{i \in I}$ sont isomorphes au corps des fractions rationnelles $\Omega(X_i)_{i \in I}$. Donc leurs clôtures algébriques sont isomorphes.

Soit Ω_p la clôture algébrique du corps premier de caractéristique p ; Ω_p est donc dénombrable. Si le cardinal $\overline{\overline{I}}$ de I est $\geqslant \aleph_0$, le cardinal du corps des fractions rationnelles $\Omega(X_i)_{i \in I}$ est égal à $\overline{\overline{I}}$, donc aussi celui de sa clôture algébrique. Donc si K est un corps algébriquement clos de caractéristique p, de puissance $2^{\aleph_0}$, les bases de transcendance de K sur Ω_p ont pour puissance $2^{\aleph_0}$. Deux corps algébriquement clos de caractéristique p, de puissance $2^{\aleph_0}$ ont donc des bases de transcendance équipotentes sur Ω_p, donc sont isomorphes. Comme les axiomes de corps algébriquement clos de caractéristique p n'ont que des modèles infinis, il suffit d'appliquer la partie *b*), avec $\aleph = 2^{\aleph_0}$ pour voir qu'ils sont saturés.

4. *a*) On rappelle que tout corps ordonné se plonge dans un corps réel fermé (voir V. d. Waerden).

Montrer que si un polynôme $p(x_1, ..., x_n)$ à coefficients dans un corps ordonné K est $\geqslant 0$ pour toutes les valeurs de $x_1, ..., x_n$ dans une extension réelle fermée de K, il est $\geqslant 0$ pour toutes les valeurs $x_1, ..., x_n$ dans toute extension ordonnée de K.

b) Un corps L est dit réel si quels que soient $x_1, ..., x_n$ dans L on a $x_1^2 + \cdots + x_n^2 + 1 \neq 0$. On rappelle que tout corps réel se plonge dans un corps réel fermé donc peut être ordonné.

Soit $a \in L$. Montrer que si a n'est pas une somme de carrés le corps $L(\sqrt{-a})$ est réel. En déduire qu'il y a un ordre sur L qui rend $a < 0$.

c) On considère un corps K réel dans lequel, pour tout élément a de K, a ou $-a$ est somme de carrés d'éléments de K. Montrer que si $p(x_1, ..., x_n)$ à coefficients dans K est $\geqslant 0$ quels que soient $x_1, ..., x_n$ dans une extension réelle fermée de K, il existe des fractions rationnelles $r_1, ..., r_k$ à coefficients dans K telles que $p = r_1^2 + \cdots + r_k^2$.

d) Soit $p(x_1, ..., x_n)$ un polynôme à coefficients dans $\mathbf{Q}$, positif ou nul pour toutes les valeurs des variables (dans $\mathbf{Q}$). Alors il existe des fractions rationnelles à coefficients dans $\mathbf{Q}$: $r_1, ..., r_k$, telles que $p = r_1^2 + \cdots + r_k^2$.

Solution. — *a*) D_K désignant le diagramme de K, et $\mathscr{A}$ les axiomes de corps réel fermé, il est immédiat que $(\mathscr{A}, D_K)$ est saturé. Comme la formule $\bigwedge x_1 ... \bigwedge x_n(p(x_1, ..., x_n) \geqslant 0)$ est satisfaite dans un des modèles de $(\mathscr{A}, D_K)$, elle est satisfaite dans tous les corps réels fermés contenant K, donc dans tous les corps ordonnés contenant K, puisqu'ils se plongent dans un corps réel fermé.

b) Tout élément de $L(\sqrt{-a})$ est de la forme $\alpha + \beta\sqrt{-a}$, avec α, $\beta \in L$. Si on a $1 + \sum_i (\alpha_i + \beta_i \sqrt{-a})^2 = 0$,

$$1 + \sum \alpha_i^2 - a \sum \beta_i^2 = 0 \,.$$

Donc

$$a = \frac{1 + \sum \alpha_i^2}{\sum \beta_i^2} = \frac{(1 + \sum \alpha_i^2) \sum \beta_i^2}{(\sum \beta_i^2)^2},$$

ce qui montre que a est une somme de carrés, ce qui est une contradiction.

c) Il est clair que K ne peut être ordonné que d'une seule façon : si a est une somme de carrés, a est positif. Sinon $a \leqslant 0$. Il en résulte que dans tout corps ordonné contenant K, on a $p(x_1, ..., x_n) \geqslant 0$. Or le corps $K(X_1, ..., X_n)$ des fractions rationnelles à n variables sur K est un corps réel. Il en résulte que $p(X_1, ..., X_n)$ (valeur du polynôme $p(x_1, ..., x_n)$ pour $x_1 = X_1, ..., x_n = X_n$, les variables X étant éléments de base du corps $K(X_1, ..., X_n)$) est $\geqslant 0$ dans tout ordre sur $K(X_1, ..., X_n)$ et par suite est une somme de carrés d'éléments de ce corps.

d) Si $p(x_1, ..., x_n) \geqslant 0$ pour $x_1, ..., x_n \in \mathbf{Q}$, comme c'est une fonction continue on a $p(x_1, ..., x_n) \geqslant 0$ dans $\mathbf{R}$. Il en suffit alors de remarquer d'une part que $\mathbf{R}$ est réel fermé, d'autre part que tout élément positif de $\mathbf{Q}$ est une somme de carrés d'éléments de $\mathbf{Q}$ pour obtenir le résultat (Théorème d'Artin).

5. *a*) $\mathscr{L}$ désigne le langage utilisé au paragraphe III et $\mathscr{L}'$ le langage obtenu en ajoutant à $\mathscr{L}$ un symbole fonctionnel à 2 variables : $\times$.

Montrer qu'il n'y a aucune formule de $\mathscr{L}$, à 3 variables libres dont la valeur dans la réalisation standard (sur $\mathbf{Z}$) de $\mathscr{L}$ soit l'ensemble :

$$\{ (m, n, p) \in \mathbf{Z}^3 : m = np \}.$$

b) Soit $\mathscr{A}$ l'ensemble des formules de $\mathscr{L}'$ satisfaites par la réalisation standard de $\mathscr{L}$ (où $\times$ est interprété comme l'opération produit) et soit $\mathscr{A}_1$ l'ensemble des formules obtenues en substituant à $\times$ dans $\mathscr{A}$ un autre symbole fonctionnel à 2 variables $\times_1$ non dans $\mathscr{L}'$. Montrer que l'ensemble $(\mathscr{A}, \mathscr{A}_1)$ a un modèle dans lequel les valeurs de $\times$ et $\times_1$ sont distinctes.

Solution. — *a*) Soit $F(x, y, z)$ une telle formule. Comme la réalisation standard satisfait les axiomes utilisés au paragraphe III, il existe une formule $G(x)$ sans quantificateurs à une variable x, telle que $G(x)$ et $\bigvee y F(x, y, y)$ prennent la même valeur dans la réalisation standard, cette valeur étant l'ensemble des carrés. Or pour toute formule $H(x)$ sans quantificateurs à une variable libre de $\mathscr{L}$, il existe deux entiers positifs N et p tels que ($\overline{H}$ désignant la valeur de $H(x)$ dans la réalisation standard) pour tout entier $n \geqslant N$, $n \in \overline{H} \Leftrightarrow n + p \in \overline{H}$: c'est évident si H est atomique (car alors H est de l'une des formes $ax + b = 0$; $ax + b > 0$; $n \mid ax + b$; avec $a, b \in \mathbf{Z}$) et il est immédiat que si H et H' ont cette propriété, $\vee HH'$ et $\neg H$ l'ont aussi. On a donc une contradiction car il n'existe pas d'en-

tiers N, p tels que si $n \geqslant N$, n est un carré si et seulement si $n+p$ en est un.

b) Supposons que dans tout modèle de $(\mathscr{A}, \mathscr{A}_1)$ les valeurs de $\times$ et $\times_1$ sont les mêmes. Alors la formule $\wedge a \wedge b[a \times b = a \times_1 b]$ est conséquence de $(\mathscr{A}, \mathscr{A}_1)$. Le théorème de définissabilité montre alors l'existence d'une formule $F(a, b, c)$ de $\mathscr{L}$ telle que $F(a, b, c) \leftrightarrow a = b \times c$ soit conséquence de $\mathscr{A}$. Comme $\mathscr{A}$ est satisfait dans la réalisation standard le $\mathscr{L}$, la valeur de F dans cette réalisation est

$$\{(m, n, p) \in \mathbf{Z}^3 : m = np\}$$

ce qui contredit le résultat précédent.

6. (*Nullstellensatz de Hilbert*). Soient K un corps et L une extension algébriquement close de K; si $p_1, ..., p_k$ sont des polynômes à n variables $x_1, ..., x_n$ à coefficients dans K, qui n'ont aucune racine commune dans L, il existe des polynômes $q_1, ..., q_k$ à n variables à coefficients dans K tels que

$$\sum_{i=1}^{k} q_i p_i = 1 .$$

Solution : Soient $\mathscr{A}$ les axiomes de corps algébriquement clos et D_K le diagramme de K. Alors $(\mathscr{A}, D_K)$ est saturé et L en est un modèle. Donc $p_1, ..., p_k$ n'ont de racine commune dans aucune extension algébriquement close de K. Comme toute extension de K se plonge dans une extension algébriquement close, on voit que $p_1, ..., p_k$ n'ont de racine commune dans aucune extension de K. Soit I l'idéal de $K[x_1, ..., x_n]$ engendré par $p_1, ..., p_k$. Si cet idéal est différent de $K[x_1, ..., x_n]$, il se plonge dans un idéal maximal J. Le quotient $K[x_1, ..., x_n]/J$ est une extension de K dans laquelle $p_1, ..., p_k$ ont une racine commune, à savoir l'image canonique de $(x_1, ..., x_n)$. Comme c'est impossible on a

$$I = K[x_1, ..., x_n],$$

donc $1 \in I$. C. q. f. d.

5. CALCUL DES PRÉDICATS A PLUSIEURS TYPES D'OBJETS ; ÉCHELLE DES TYPES FINIS

Résumé

La première partie de ce chapitre et l'exercice 1 exposent une seconde méthode — annoncée dans le résumé du chapitre 2 — pour développer la logique des prédicats du premier ordre. Les résultats essentiels sont formulés et démontrés directement pour les langages avec plusieurs espèces de variables, lesquels sont couramment employés en mathématiques. L'emploi de tels langages est, en principe, réductible à celui de langages avec une seule espèce de variables et des prédicats monadiques $M_i(x)$ signifiant « x appartient à l'espèce i ». Mais, en pratique, ces langages sont utiles parce qu'ils permettent de formuler simplement certains résultats, par exemple, une forme améliorée du lemme d'interpolation, qui sera fort utile dans le prochain chapitre. La construction de modèles canoniques indiquée dans ce chapitre est en pratique beaucoup plus commode pour les langages avec plusieurs espèces de variables que celle du chapitre 2 ; voir l'exercice 2 pour la relation entre ces deux méthodes.

La seconde partie étudie les langages, toujours à plusieurs sortes de variables qui sont ainsi constitués : une espèce pour les individus, une pour les ensembles d'individus, une pour les familles de tels ensembles, et ainsi de suite par itération finie. Ces langages ont été rendus familiers par les mathématiques axiomatiques où, par exemple, dans la théorie des groupes, les éléments du groupe considéré jouent le rôle d'individus tandis que les sous-groupes sont des *ensembles* de tels individus (ensembles sur lesquels on prend la restriction de l'opération de groupe). Plus généralement, les langages considérés ici sont ceux obtenus aux niveaux finis de la structure ou « échelle » des types (simples). L'exercice 5 définit la structure des types cumulatifs et donne sa relation avec la structure des types simples.

Dans la classe de réalisations que nous considérons ici (celle des modèles généraux), le domaine C_0 des variables d'individus est quelconque et les domaines des autres variables sont des familles d'ensembles incluses respectivement dans les types 1, 2, ... de l'échelle ayant pour base C_0, et soumises seulement à certaines conditions de clôture. L'étude de ces réalisations générales est réductible au chapitre 2 (grâce aux axiomes d'extensionnalité). Deux autres classes de réalisations seront traitées dans le dernier chapitre.

Un langage $\mathscr{L}$ à k types d'objets est, par définition, constitué par :

1° k ensembles infinis disjoints $V_{\mathscr{L}}^{(1)}, ..., V_{\mathscr{L}}^{(k)}$. Les éléments de $V_{\mathscr{L}}^{(i)}$ $(1 \leqslant i \leqslant k)$ sont appelés variables de type i de $\mathscr{L}$.

2° k ensembles disjoints $C_{\mathscr{L}}^{(1)}, ..., C_{\mathscr{L}}^{(k)}$. Les éléments de $C_{\mathscr{L}}^{(i)}$ $(1 \leqslant i \leqslant k)$ sont appelés symboles de constante de type i de $\mathscr{L}$.

3° Pour chaque entier $n \geqslant 0$, un ensemble $\mathrm{R}_{\mathscr{L}}^{(n)}$ dont les éléments sont appelés symboles relationnels à n variables (de type quelconque).

4° Pour chaque suite $(i_1, ..., i_n)$ formée d'entiers compris entre 1 et k, un ensemble $\mathrm{S}_{\mathscr{L}}^{(i_1, ..., i_n)}$ dont les éléments sont appelés symboles relationnels de type $(i_1, ..., i_n)$ (ou symboles relationnels à n variables dont la première est de type i_1, ..., la n-ième de type i_n).

Tous ces ensembles sont supposés disjoints deux à deux.

Les formules atomiques sont, par définition, les suites de symboles de $\mathscr{L}$ de l'une des deux formes suivantes :

a) $R\xi_1 ... \xi_n$, où R est un symbole relationnel à n variables $(R \in \mathrm{R}_{\mathscr{L}}^{(n)})$, et où $\xi_1, ..., \xi_n$ sont des variables ou des symboles de constante de $\mathscr{L}$ de type quelconque :

$$\xi_i \in \bigcup_{j=1}^{k} C_{\mathscr{L}}^{(j)} \cup V_{\mathscr{L}}^{(j)} \qquad \text{pour} \qquad 1 \leqslant i \leqslant n\,.$$

b) $\xi S_1^{(i_1)} ... \xi_n^{(i_n)}$, où S est un symbole relationnel de type $(i_1, ..., i_n)$ $(S \in \mathrm{S}_{\mathscr{L}}^{(i_1, ..., i_n)})$ et où $\xi_1^{(i_1)}$ est une variable ou un symbole de constante de type i_1, ..., $\xi_n^{(i_n)}$ une variable ou un symbole de constante de type i_n.

L'ensemble des formules atomiques de $\mathscr{L}$ sera désigné par $At_{\mathscr{L}}$.

L'ensemble $\mathscr{F}_{\mathscr{L}}$ des formules de $\mathscr{L}$, est par définition, l'ensemble des schémas fonctionnels construits avec les formules atomiques de $\mathscr{L}$ comme symboles à 0 variables, $\neg$ et $\forall x$ comme symboles à 1 variable (x décrivant $V_{\mathscr{L}}^{(1)} \cup \cdots \cup V_{\mathscr{L}}^{(k)}$), $\vee$ comme symbole à 2 variables (voir préliminaires).

On définit comme au chapitre 2 les notations $\wedge x$, $\rightarrow$, $\leftrightarrow$; les variables libres d'une formule de $\mathscr{L}$; la notion de formule close de $\mathscr{L}$.

Une réalisation du langage $\mathscr{L}$ à k types d'objets est, par définition, constituée par :

1° k ensembles non vides $E_1, ..., E_k$; E_i $(1 \leqslant i \leqslant k)$ est appelé ensemble de base de type i de la réalisation.

2° Pour chaque i $(1 \leqslant i \leqslant k)$ une application $c \rightarrow \bar{c}$ de $C_{\mathscr{L}}^{(i)}$ dans E_i.

3° Pour chaque entier $n \geqslant 0$ une application $R \rightarrow \bar{R}$ de $\mathrm{R}_{\mathscr{L}}^{(n)}$ dans

$$\mathfrak{P}[(E_1 \cup \cdots \cup E_k)^n].$$

4° Pour chaque suite $(i_1, ..., i_n)$ d'entiers compris entre 1 et k, une application $S \rightarrow \bar{S}$ de $\mathrm{S}_{\mathscr{L}}^{(i_1, ..., i_n)}$ dans $\mathfrak{P}[E_{i_1} \times \cdots \times E_{i_n}]$.

La valeur $\overline{F}$ prise par une formule F de $\mathscr{L}$ dans cette réalisation est un sous-ensemble de $E_1^{V_{\mathscr{L}}^{(1)}} \times \cdots \times E_k^{V_{\mathscr{L}}^{(k)}}$ (ensemble des suites $(\delta_1, ..., \delta_k)$, où δ_i est une application de $V_{\mathscr{L}}^{(i)}$ dans E_i ; c'est donc aussi l'ensemble des applications δ de $\bigcup_{j=1}^{k} V_{\mathscr{L}}^{(j)}$ dans $\bigcup_{j=1}^{k} E_j$ telles que $\delta(V_{\mathscr{L}}^{(j)}) \subset E_j$ pour $1 \leqslant j \leqslant k$, puisque $V_{\mathscr{L}}^{(1)}, ..., V_{\mathscr{L}}^{(k)}$ sont disjoints). On la définit de la façon suivante :

— Si F est une formule atomique, elle est de la forme $R\xi_1^{(i_1)} ... \xi_n^{(i_n)}$ avec $R \in \mathrm{R}_{\mathscr{L}}^{(n)}$ ou $R \in \mathrm{S}_{\mathscr{L}}^{(i_1, ..., i_n)}$, $\xi_1^{(i_1)}, ..., \xi_n^{(i_n)}$ étant des variables ou des symboles de constante de types respectifs $i_1, ..., i_n$; la valeur $\overline{F}$ prise par F est alors l'ensemble des

$$\delta \in E_1^{V_{\mathscr{L}}^{(1)}} \times \cdots \times E_k^{V_{\mathscr{L}}^{(k)}}$$

telles que

$$(\delta'(\xi_1^{(i_1)}), ..., \delta'(\xi_n^{(i_n)})) \in \overline{R},$$

ou $\delta'(\xi_j^{(i)}) = \delta(\xi_j^{(i)})$ si $\xi_j^{(i)}$ est une variable, et

$\delta'(\xi_j^{(i)}) = \overline{\xi_j^{(i)}}$ si $\xi_j^{(i)}$ est un symbole de constante.

— D'après le théorème sur les schémas fonctionnels (voir préliminaires), $\overline{F}$ est alors défini pour chaque formule F si on pose $\overline{F \vee G} = \overline{F} \cup \overline{G}$; $\overline{\neg F} = \complement \overline{F}$; $\overline{\forall x F}$ = projection de $\overline{F}$ suivant la variable x (c'est l'ensemble des

$$\delta \in E_1^{V_{\mathscr{L}}^{(1)}} \times \cdots \times E_k^{V_{\mathscr{L}}^{(k)}}$$

telles qu'il existe $\delta_1 \in \overline{F}$, δ_1 étant égale à δ pour toute variable sauf peut-être x).

De même qu'au chapitre 2 on voit que la valeur prise par une formule close F est soit $E_1^{V_{\mathscr{L}}^{(1)}} \times \cdots \times E_k^{V_{\mathscr{L}}^{(k)}}$ soit ϕ.

Dans le premier cas on dit que F est satisfaite par la réalisation considérée. Si $\mathscr{A}$ est un ensemble de formules closes de $\mathscr{L}$, on dit que la formule F est conséquence de $\mathscr{A}$, et on écrit $\mathscr{A} \vdash F$, si toute réalisation de $\mathscr{L}$ qui satisfait $\mathscr{A}$ (c'est-à-dire qui satisfait chaque formule de $\mathscr{A}$) satisfait aussi F. Un théorème de $\mathscr{L}$ est par définition une formule dont la clôture est satisfaite par toutes les réalisations de $\mathscr{L}$.

De même qu'au chapitre 2, on définit les formules prénexes de $\mathscr{L}$, et on montre que toute formule de $\mathscr{L}$ équivaut à une formule prénexe.

Une réalisation de $\mathscr{L}$ sera dite *canonique* si son ensemble de base de type i est $C_{\mathscr{L}}^{(i)}$ (ensemble des symboles de constante de type i de $\mathscr{L}$) pour $1 \leqslant i \leqslant k$, et si pour chaque symbole de constante c de $\mathscr{L}$ on a $\overline{c} = c$ dans cette réalisation. Remarquons que si l'un des ensembles $C_{\mathscr{L}}^{(i)}$ est vide, $\mathscr{L}$ n'a pas de réalisation canonique.

A toute réalisation canonique de $\mathscr{L}$ correspond une réalisation du calcul propositionnel construit sur les formules atomiques closes de $\mathscr{L}$: la valeur prise par $Ra_1^{(i_1)} \dots a_n^{(i_n)}$ (où R est un symbole relationnel à n variables, ou un symbole relationnel de type $(i_1, \dots, i_n)$, et où $a_1^{(i_1)}, \dots, a_n^{(i_n)}$ sont des symboles de constante de types respectifs $i_1, \dots, i_n$) étant 1 ou 0 suivant que $(a_1^{(i_1)}, \dots, a_n^{(i_n)})$ appartient ou non à $\bar{R}$.

Inversement toute réalisation du calcul propositionnel construit sur les formules atomiques closes de $\mathscr{L}$ définit de cette façon une réalisation canonique de $\mathscr{L}$.

Le lemme suivant se vérifie immédiatement par récurrence sur la longueur de F :

LEMME 1. — *Soit F une formule du langage $\mathscr{L}$, close, sans quantificateurs. Alors F est toujours simultanément satisfaite ou non satisfaite par une réalisation canonique de $\mathscr{L}$ et la réalisation correspondante du calcul propositionnel construit sur les formules atomiques closes de $\mathscr{L}$.*

Soient $\Delta_n^{(i)}$ ($1 \leqslant i \leqslant k$; n entier $\geqslant 1$) une famille d'ensembles disjoints, ayant chacun le même cardinal que l'ensemble des formules de $\mathscr{L}$, et disjoints de $\mathscr{L}$ (aucun élément de $\Delta_n^{(i)}$ n'est une variable ou un symbole de $\mathscr{L}$). Posons $\Delta^{(i)} = \bigcup_{n \geqslant 1} \Delta_n^{(i)}$ et soit $\mathscr{L}_\Delta$ le langage obtenu en ajoutant à $\mathscr{L}$ chaque élément de $\Delta^{(i)}$ comme symbole de constante de type i. L'ensemble des symboles de constante de type i de $\mathscr{L}_\Delta$ est donc $C_{\mathscr{L}}^{(i)} \cup \Delta^{(i)}$. On pose :

$$\Delta_n = \bigcup_{1 \leqslant i \leqslant k} \Delta_n^{(i)} \qquad \text{et} \qquad \Delta = \bigcup_{n \geqslant 1} \Delta_n = \bigcup_{1 \leqslant i \leqslant k} \Delta^{(i)}.$$

Pour chaque $a \in \Delta^{(i)}$, l'entier n tel que $a \in \Delta_n^{(i)}$ est appelé *le rang de a* (l'entier i compris entre 1 et k étant le type de a). *Le rang d'une formule F* de $\mathscr{L}_\Delta$ est par définition le maximum des rangs des éléments de Δ qui y figurent, ou 0 s'il n'y figure aucun élément de Δ, c'est-à-dire si F est une formule de $\mathscr{L}$.

Pour chaque i ($1 \leqslant i \leqslant k$) on choisit une variable $x^{(i)}$ de $\mathscr{L}$, de type i, et on désigne par $\mathscr{F}_n^{(i)}$ l'ensemble des formules de rang n de $\mathscr{L}_\Delta$ ayant $x^{(i)}$ pour seule variable libre. Il est clair que $\mathscr{F}_n^{(i)}$ et $\Delta_{n+1}^{(i)}$ ont même cardinal (qui est celui de l'ensemble des formules de $\mathscr{L}$). Pour chaque couple (i, n) (avec $1 \leqslant i \leqslant k$ et n entier $\geqslant 0$) on se donne une bijection ε de $\mathscr{F}_n^{(i)}$ sur $\Delta_{n+1}^{(i)}$. Pour chaque $a \in \Delta^{(i)}$, il existe donc une formule $A(x^{(i)})$ et une seule, ayant $x^{(i)}$ pour seule variable libre, et telle que $a = \varepsilon A(x^{(i)})$; de plus le rang de $A(x^{(i)})$ est inférieur d'une unité à celui de a.

On désigne par Ω_a la formule $\forall x^{(i)} A(x^{(i)}) \rightarrow A(a)$ pour $a = \varepsilon A(x^{(i)})$; par $\Omega_n^{(i)}$ l'ensemble des Ω_a pour $a \in \Delta_n^{(i)}$, par $\Omega^{(i)}$ l'ensemble des Ω_a pour $a \in \Delta^{(i)}$, par Ω_n l'ensemble des Ω_a pour $a \in \Delta_n$, et par Ω l'ensemble des Ω_a pour $a \in \Delta$.

On a donc

$$\Omega = \bigcup_{n \geq 1} \Omega_n = \bigcup_{1 \leq i \leq k} \Omega^{(i)}.$$

PROPOSITION 1. — *Toute réalisation de $\mathscr{L}$ s'étend à $\mathscr{L}_\Delta$ en un modèle de Ω.*

Soit $\mathfrak{M}$ une réalisation de $\mathscr{L}$, d'ensembles de base $E_1, ..., E_k$. On définit la valeur $\bar{a}$ de $a \in \Delta$ par récurrence sur le rang de a : supposons défini $\bar{b}$ pour chaque $b \in \bigcup_{p<n} \Delta_p$, de façon que $\Omega_1, \Omega_2, ..., \Omega_{n-1}$ soient satisfaits.

Soit $a \in \Delta_n$; la formule $A(x)$ telle que $a = \varepsilon A(x)$ est de rang $n - 1$, et par suite a une valeur $\overline{A(x)}$ dans la réalisation de $\mathscr{L} \cup \Delta_1 \cup \cdots \cup \Delta_{n-1}$ ainsi définie. Si $\overline{A(x)} \neq \phi$, il existe $\alpha \in E_i$ (i est le type de a) tel que $\alpha \in \overline{A(x)}$. On pose alors $\bar{a} = \alpha$; si $\overline{A(x)} = \phi$ on pose $\bar{a}$ = un élément quelconque de E_i. Dans les deux cas Ω_a, qui est $\bigvee x A(x) \rightarrow A(a)$, est satisfaite. C. q. f. d.

PROPOSITION 2. — *Pour tout modèle $\mathfrak{M}$ de Ω, il existe un modèle canonique $\mathfrak{M}_1$, satisfaisant les mêmes formules closes de $\mathscr{L}_\Delta$ que $\mathfrak{M}$.*

Soit R un symbole relationnel à n variables, ou un symbole relationnel de type $(i_1, ..., i_n)$ de $\mathscr{L}$, et soit $\overline{R}_{\mathfrak{M}}$ la valeur qu'il prend dans la réalisation donnée $\mathfrak{M}$. On définit $\overline{R}_{\mathfrak{M}_1}$, valeur de R dans la réalisation $\mathfrak{M}_1$, en posant

$$\overline{R}_{\mathfrak{M}_1} = \{ (a_1, ..., a_n) \text{ ; la formule } Ra_1 ... a_n \text{ est satisfaite dans } \mathfrak{M} \}.$$

(Si R est un symbole relationnel de type $(i_1, ..., i_n)$, $a_1, ..., a_n$ sont de types respectifs $i_1, ..., i_n$ sinon $Ra_1 ... a_n$ n'est pas une formule de $\mathscr{L}$).

Soit F une formule close de $\mathscr{L}_\Delta$. On va montrer, par récurrence sur la longueur de F, qu'elle est simultanément satisfaite ou non satisfaite par $\mathfrak{M}$ et $\mathfrak{M}_1$. C'est évident si F est atomique par définition de $\mathfrak{M}_1$.

— Si $F = \neg G$, d'après l'hypothèse de récurrence, G est, par exemple, satisfaite par $\mathfrak{M}$ et $\mathfrak{M}_1$: donc F est non satisfaite par $\mathfrak{M}$ et $\mathfrak{M}_1$. De même si $F = G \vee H$.

— Si $F = \bigvee x G(x)$, supposons d'abord F satisfaite par $\mathfrak{M}$. Comme $\mathfrak{M}$ satisfait Ω, $\mathfrak{M}$ satisfait $G(g)$, où $g = \varepsilon G(x)$: car Ω contient la formule $\bigvee x G(x) \rightarrow G(g)$. D'après l'hypothèse de récurrence, $\mathfrak{M}_1$ satisfait aussi $G(g)$ et donc satisfait F. Si maintenant $\mathfrak{M}$ ne satisfait pas F, $\mathfrak{M}$ satisfait toutes les formules $\neg G(a)$, où a décrit l'ensemble des symboles de constante de $\mathscr{L}_\Delta$ de même type que x. D'après l'hypothèse de récurrence, $\mathfrak{M}_1$ satisfait aussi ces formules ; mais comme l'ensemble de base de type i de $\mathfrak{M}_1$ est l'ensemble des symboles de constante de type i de $\mathscr{L}_\Delta$, $\mathfrak{M}_1$ satisfait $\bigwedge x \neg G(x)$, c'est-à-dire $\neg F$.

C. q. f. d.

A chaque formule F de $\mathscr{L}_\Delta$, prénexe, close, associons un ensemble $\langle F \rangle$ de formules closes sans quantificateur de $\mathscr{L}_\Delta$, défini par récurrence sur la longueur de F de la façon suivante :

— si F est sans quantificateur, $\langle F \rangle = \{ F \}$ (ensemble réduit à F).
— si F est $\bigvee x G(x)$, alors $\langle F \rangle = \langle G(g) \rangle$ où $g = \varepsilon G(x)$.
— si F est $\bigwedge x G(x)$, alors $\langle F \rangle = \bigcup_a \langle G(a) \rangle$, où a décrit l'ensemble des symboles de constante de $\mathscr{L}_\Delta$ de même type que x.

Lemme 2. — *Tout modèle canonique de $\langle F \rangle$ satisfait F ; tout modèle de (Ω, F) satisfait $\langle F \rangle$ (autrement dit $\Omega, F \vdash \langle F \rangle$).*

Démonstration par récurrence sur la longueur de F. Le lemme est évident si F est sans quantificateur puisqu'alors $\langle F \rangle = \{ F \}$.

Si F est $\bigvee x G(x)$, soit $\mathfrak{M}$ un modèle canonique de $\langle F \rangle$, c'est-à-dire de $\langle G(g) \rangle$, avec $g = \varepsilon G(x)$. Comme $G(g)$ est plus courte que F, $\mathfrak{M}$ satisfait $G(g)$, donc aussi F. D'autre part, $\Omega, F \vdash \Omega, \bigvee x G(x) \to G(g), \bigvee x G(x)$. Donc $\Omega, F \vdash \Omega, G(g)$. D'après l'hypothèse de récurrence $\Omega, G(g) \vdash \langle G(g) \rangle$ ce qui montre que $\Omega, F \vdash \langle F \rangle$.

Si F est $\bigwedge x G(x)$, soit $\mathfrak{M}$ un modèle canonique de $\langle F \rangle$ donc de $\bigcup_a \langle G(a) \rangle$ (où a décrit l'ensemble des symboles de constante de $\mathscr{L}_\Delta$ de même type que x). L'hypothèse de récurrence entraîne que $\mathfrak{M}$ satisfait chacune des formules $G(a)$; comme $\mathfrak{M}$ est une réalisation canonique, elle satisfait $\bigwedge x G(x)$. D'autre part, $\Omega, F \vdash \Omega, G(a)$ pour chaque symbole de constante a de même type que x. D'après l'hypothèse de récurrence, $\Omega, G(a) \vdash \langle G(a) \rangle$; donc $\Omega, F \vdash \bigcup_a \langle G(a) \rangle$ c'est-à-dire $\Omega, F \vdash \langle F \rangle$. C. q. f. d.

Théorème 1 (théorème de finitude). — *Si tout sous-ensemble fini d'un ensemble $\mathscr{A}$ de formules closes de $\mathscr{L}$ a un modèle, $\mathscr{A}$ a un modèle.*

On peut supposer $\mathscr{A}$ formé de formules prénexes closes. Désignons alors par $\mathscr{B}$ la réunion des $\langle F \rangle$ pour $F \in \mathscr{A}$. Soit U un sous-ensemble fini quelconque de $\mathscr{B}$; on a donc $U \subset \langle F_1 \rangle \cup \cdots \cup \langle F_n \rangle$. Comme $(F_1, ..., F_n)$ a un modèle par hypothèse, $(\Omega, F_1, ..., F_n)$ en a un (proposition 1), donc a un modèle canonique (proposition 2). Comme $\Omega, F_i \vdash \langle F_i \rangle$ (lemme 2), ce modèle satisfait $\langle F_1 \rangle, \langle F_2 \rangle, ..., \langle F_n \rangle$, donc aussi U. Tout sous-ensemble fini U de $\mathscr{B}$ a donc un modèle canonique, donc aussi un modèle au sens du calcul propositionnel construit sur les formules atomiques closes de $\mathscr{L}_\Delta$ (lemme 1). Le théorème de finitude pour le calcul propositionnel montre alors que $\mathscr{B}$ a un modèle au sens du calcul propositionnel, donc (lemme 1) un modèle canonique. Celui-ci satisfait $\langle F \rangle$ pour chaque $F \in \mathscr{A}$, donc satisfait $\mathscr{A}$ d'après le lemme 2.

C. q. f. d.

Corollaire. — *Soient I un ensemble totalement ordonné et $(\mathscr{A}_i)_{i \in I}$ une*

famille croissante d'ensembles de formules closes de $\mathscr{L}$ $(i \leqslant j \Rightarrow \mathscr{A}_i \subset A_j)$. Si chaque $\mathscr{A}_i$ possède un modèle, $\bigcup_{i \in I} \mathscr{A}_i$ en a un.

Il suffit en effet de montrer que tout sous-ensemble fini $(F_1, ..., F_n)$ de $\bigcup_{i \in I} \mathscr{A}_i$ a un modèle. Or $F_1 \in \mathscr{A}_{i_1}, ..., F_n \in \mathscr{A}_{i_n}$. Si i_n par exemple est le plus grand élément de la suite $(i_1, ..., i_n)$ on a $(F_1, ..., F_n) \subset \mathscr{A}_{i_n}$ et donc $(F_1, ..., F_n)$ a un modèle.

C. q. f. d.

— A chaque formule F prénexe close de $\mathscr{L}_\Delta$, associons un sous-ensemble $\Delta(F)$ de Δ, défini par récurrence sur la longueur de F de la façon suivante :

— si F est sans quantificateur, $\Delta(F) = \phi$,

— si F est $\bigvee x\, G(x)$, alors $\Delta(F) = \Delta(G(g)) \cup \{ g \}$ (où $g = \varepsilon G(x)$).

— si F est $\bigwedge x G(x)$, alors $\Delta(F) = \bigcup_a \Delta(G(a))$, où a décrit l'ensemble des symboles de constante de $\mathscr{L}_\Delta$ de même type que x.

Désignons par $\Omega(F)$ l'ensemble des formules Ω_a pour $a \in \Delta(F)$.

Le lemme suivant précise la deuxième partie du lemme 2 :

LEMME 3. — *Pour chaque formule F prénexe close de $\mathscr{L}_\Delta$, $\langle F \rangle$ est conséquence de $(\Omega(F), F)$.*

Démonstration par récurrence sur la longueur de F. Le lemme est évident si F est sans quantificateur, car $\Omega(F) = \phi$ et $\langle F \rangle = \{ F \}$.

Si F est $\bigvee x G(x)$, on a $\langle F \rangle = \langle G(g) \rangle$, avec $g = \varepsilon G(x)$. D'après l'hypothèse de récurrence, $\langle F \rangle$ est conséquence de $\Omega(G(g))$, $G(g)$. Or $\Omega(F)$ contient $\Omega(G(g))$ et Ω_g ; de plus $F, \Omega_g \vdash G(g)$. Donc $\Omega(F), F \vdash \langle G(g) \rangle$ et par suite $\Omega(F), F \vdash \langle F \rangle$.

Si F est $\bigwedge x G(x)$, soit $U \in \langle F \rangle$; alors $U \in \langle G(a) \rangle$ pour un certain symbole de constante a de même type que x. D'après l'hypothèse de récurrence, $\Omega(G(a)), G(a) \vdash \langle G(a) \rangle$, donc $\Omega(G(a)), G(a) \vdash U$. Comme $\Omega(F) \supset \Omega(G(a))$ et que $F \vdash G(a)$, on a bien $\Omega(F), F \vdash U$.

C. q. f. d.

LEMME 4. — *Si F et G sont deux formules prénexes closes de $\mathscr{L}_\Delta$ telles que $\Delta(F) \cap \Delta(G) \neq \phi$, F et G ont les mêmes symboles relationnels et les mêmes types.*

Soit $b \in \Delta(F) \cap \Delta(G)$. Comme $b \in \Delta$, on a $b = \varepsilon B(x)$, pour une certaine formule $B(x)$ à une variable libre. On montre par récurrence sur la longueur de F, que F et $B(x)$ ont les mêmes symboles relationnels et les mêmes types.

F ne peut être sans quantificateur, sinon $\Delta(F)$ serait vide. Si F est $\bigvee x G(x)$, comme $b \in \Delta(F)$ on a $b \in \Delta(G(g)) \cup \{ g \}$ (où $g = \varepsilon G(x)$). Si $b \in \Delta(G(g))$, d'après l'hypothèse de récurrence $G(g)$ et $B(x)$ ont les mêmes symboles relationnels et les mêmes types, donc aussi F et $B(x)$; si $b = g$ alors $B(x) = G(x)$

(car ε est biunivoque) donc F et $B(x)$ ont les mêmes symboles relationnels et les mêmes types.

Si F est $\bigwedge xG(x)$, comme $b \in \Delta(F)$, on a $b \in \Delta(G(a))$ pour un certain symbole de constante a de même type que x. D'après l'hypothèse de récurrence, $G(a)$ et $B(x)$ ont les mêmes symboles relationnels et les mêmes types, donc aussi F et $B(x)$.

On montre de même que G et $B(x)$ ont les mêmes symboles relationnels et les mêmes types, donc aussi F et G.

C. q. f. d.

THÉORÈME 2 (THÉORÈME D'INTERPOLATION). — *Soient F et G deux formules closes de $\mathscr{L}$, telles que $F \wedge G$ n'ait pas de modèle. Alors il existe une formule H de $\mathscr{L}$, dont les symboles relationnels et les types sont communs à F et à G, telle que $F \rightarrow H$ et $G \rightarrow \neg H$ soient deux théorèmes.*

Comme (F, G) n'a pas de modèle, $\langle F \rangle \cup \langle G \rangle$ n'a pas de modèle canonique (lemme 2), donc est contradictoire au sens du calcul propositionnel construit sur les formules atomiques closes de $\mathscr{L}_\Delta$ (lemme 1). Le lemme d'interpolation pour ce calcul propositionnel donne alors une formule C de $\mathscr{L}_\Delta$, close, sans quantificateur, dont les formules atomiques sont communes à $\langle F \rangle$ et à $\langle G \rangle$, et telle que $\langle F \rangle \vdash C$ et $\langle G \rangle \vdash \neg C$. Or les symboles relationnels et les types qui apparaissent dans $\langle F \rangle$ (resp. $\langle G \rangle$) sont ceux de F (resp. G) comme on le voit immédiatement sur la définition de $\langle F \rangle$ et $\langle G \rangle$. Il en résulte que les symboles relationnels et les types de C sont communs à F et à G. D'après le lemme 3, $\Omega(F)$, $F \vdash C$ et $\Omega(G)$, $G \vdash \neg C$.

Si $\Delta(F) \cap \Delta(G) \neq \phi$, F et G ont les mêmes symboles relationnels et les mêmes types (lemme 4). Le théorème à démontrer est trivial dans ce cas : il suffit de poser $H = F$. On peut donc supposer $\Delta(F) \cap \Delta(G) = \phi$.

D'après le théorème de finitude, on a :

$$\Omega_{a_1}, \ldots, \Omega_{a_n}, F \vdash C \tag{1}$$

$$\Omega_{b_1}, \ldots, \Omega_{b_p}, G \vdash \neg C \tag{2}$$

où $a_1, \ldots, a_n$ sont des éléments distincts de $\Delta(F)$, et $b_1, \ldots, b_p$ des éléments distincts de $\Delta(G)$. Comme $\Delta(F) \cap \Delta(G) = \phi$ on a

$$a_i \neq b_j \ (1 \leqslant i \leqslant n \, ; \ 1 \leqslant j \leqslant p) \, .$$

Soit a_n par exemple l'un des éléments de rang maximum de l'ensemble $\{ a_1, \ldots, a_n, b_1, \ldots, b_p \}$. Alors $\Omega_{a_1}, \Omega_{a_2}, \ldots, \Omega_{a_{n-1}}, \Omega_{b_1}, \Omega_{b_2}, \ldots, \Omega_{b_p}$ ne contiennent pas a_n. Soit $C_1(z)$ la formule obtenue en remplaçant a_n dans C par une variable z de même type. On a donc $C = C_1(a_n)$ et par suite $C \vdash \bigvee zC_1(z)$. Donc

$$\Omega_{a_1}, \ldots, \Omega_{a_n}, F \vdash \bigvee zC_1(z) \, .$$

Or $\Omega_{a_1}, \ldots, \Omega_{a_{n-1}}$, F, $\bigvee z C_1(z)$ ne contiennent pas a_n. D'autre part Ω_{a_n} s'écrit $\bigvee x A(x) \to A(a_n)$, où $A(x)$ ne contient pas a_n. Donc

$$\Omega_{a_1}, \ldots, \Omega_{a_{n-1}}, \bigvee y[\bigvee x A(x) \to A(y)], F \vdash \bigvee z C_1(z),$$

c'est-à-dire

$$\Omega_{a_1}, \ldots, \Omega_{a_{n-1}}, F \vdash \bigvee z C_1(z). \tag{3}$$

D'autre part :

$$\Omega_{b_1}, \ldots, \Omega_{b_p}, G \vdash \neg C_1(a_n).$$

Comme a_n n'apparaît pas dans $\Omega_{b_1}, \ldots, \Omega_{b_p}$, G, on en déduit :

$$\Omega_{b_1}, \ldots, \Omega_{b_p}, G \vdash \bigwedge z \neg C_1(z). \tag{4}$$

On recommence cette opération à partir de (3) et (4) au lieu de (1) et (2) et ainsi de suite. On élimine ainsi une par une chaque formule

$$\Omega_{a_i}, \Omega_{b_j} \quad (1 \leqslant i \leqslant n ; 1 \leqslant j \leqslant p).$$

Au $(n + p)$-ième pas on obtient une formule H, qui a les mêmes symboles relationnels et les mêmes types que C, telle que $F \vdash H$ et $G \vdash \neg H$.

C. q. f. d.

La définition et les deux lemmes qui suivent (lemmes 5 et 6) seront utilisés dans les chapitres suivants.
Pour chaque $a \in \Delta$, nous désignerons par θ_a l'intersection de tous les sous-ensembles X de Ω ayant les propriétés suivantes :

1) $\Omega_a \in X$,
2) si $b \in \Delta$, et si b apparaît dans une formule de X, alors $\Omega_b \in X$.

θ_a est donc le plus petit sous-ensemble de Ω ayant ces deux propriétés.

LEMME 5. — *Soient $a_1, \ldots, a_n$ les éléments de Δ différents de a, qui apparaissent dans Ω_a. Alors*

$$\theta_a = \theta_{a_1} \cup \theta_{a_2} \cup \cdots \cup \theta_{a_n} \cup \{ \Omega_a \}.$$

Il est clair que $\theta_{a_1} \cup \cdots \cup \theta_{a_n} \cup \{ \Omega_a \}$ a les propriétés 1 et 2 ci-dessus donc contient θ_a. Mais inversement θ_a contient Ω_{a_i} $(1 \leqslant i \leqslant n)$ et donc θ_a a les deux propriétés définissant θ_{a_i}. Donc $\theta_a \supset \theta_{a_i}$ et par suite

$$\theta_a \supset \theta_{a_1} \cup \cdots \cup \theta_{a_n} \cup \{ \Omega_a \}. \qquad \text{C. q. f. d.}$$

On en déduit que θ_a *est un sous-ensemble fini de Ω pour tout $a \in \Delta$* : c'est évident si $a \in \Delta_1$ car alors $\theta_a = \{ \Omega_a \}$; ayant montré que θ_a est fini pour tout $a \in \Delta$ de rang $< n$, le lemme précédent montre que θ_a est fini pour tout $a \in \Delta_n$.

LEMME 6. — *Soit F une formule close de $\mathscr{L}_\Delta$, $a_1, \ldots, a_n$ les éléments de Δ qui y figurent. Si $\Omega \vdash F$, alors $\theta_{a_1}, \ldots, \theta_{a_n} \vdash F$.*

D'après le théorème de finitude il existe un sous-ensemble fini Ω' de Ω tel que $\Omega' \vdash F$. Parmi les sous-ensembles finis de Ω contenant $\theta_{a_1}, ..., \theta_{a_n}$ et ayant F pour conséquence, soit

$$\Omega_0 = \theta_{a_1} \cup \cdots \cup \theta_{a_n} \cup \{ \Omega_{b_1}, ..., \Omega_{b_p} \}$$

un de ceux qui ont le plus petit nombre de formules. Supposons $p \neq 0$, et $b_1, ..., b_p$ rangés par ordre de rang non décroissant. Soit $B_p(x)$ la formule telle que $\varepsilon B_p(x) = b_p$. Alors

$$\theta_{a_1}, ..., \theta_{a_n}, \Omega_{b_1}, ..., \Omega_{b_{p-1}}, \ \mathsf{V}xB_p(x) \to B_p(b_p) \vdash F .$$

Or b_p n'apparaît pas dans $\theta_{a_i} (1 \leqslant i \leqslant n)$. Sinon d'après la définition de θ_{a_i} on aurait $\Omega_{b_p} \in \theta_{a_i}$ et Ω_{b_p} serait superflu. D'autre part b_p n'apparaît pas dans $\Omega_{b_1}, ..., \Omega_{b_{p-1}}$. Sinon, comme $b_p \neq b_1, ..., b_p \neq b_{p-1}$, le rang de b_p serait strictement inférieur au rang de l'un des b_j $(1 \leqslant j \leqslant p - 1)$. Enfin b_p n'apparaît pas dans F, car les seuls éléments de Δ qui figurent dans F sont $a_1, ..., a_n$, et on a déjà vu que b_p ne peut être l'un d'eux. Il en résulte que

$$\theta_{a_1}, ..., \theta_{a_n}, \Omega_{b_1}, ..., \Omega_{b_{p-1}}, \ \mathsf{V}y[\mathsf{V}xB_p(x) \to B_p(y)] \vdash F .$$

Donc

$$\theta_{a_1}, ..., \theta_{a_n}, \Omega_{b_1}, ..., \Omega_{b_{p-1}} \vdash F$$

et cela contredit la propriété de minimum de Ω_0. On a donc $p = 0$.

C. q. f. d.

Le calcul des prédicats à k types d'objets avec égalité.

Un langage $\mathscr{L}$ à k types d'objets est dit égalitaire si on a distingué un symbole relationnel E de $\mathscr{L}$ à 2 variables ($E \in \mathrm{R}^{(2)}_{\mathscr{L}}$).

$\mathscr{L}$ étant un langage égalitaire, ξ, η étant deux variables ou symboles de constante (de types quelconques), la formule atomique $E\xi\eta$ sera écrite $\xi = \eta$.

Une réalisation de $\mathscr{L}$, l'ensembles de base $U_1, ..., U_k$ sera dite égalitaire si la valeur de E dans cette réalisation est la diagonale de $(U_1 \cup \cdots \cup U_k)^2$ (ensemble des couples (u, u) pour $u \in U_1 \cup \cdots \cup U_k$).

Une formule close F est dite conséquence égalitaire d'un ensemble $\mathscr{A}$ de formules closes de $\mathscr{L}$ (ce que nous écrirons $\mathscr{A} \models F$, ou bien $\mathscr{A} \vdash F$ s'il n'y a pas de confusion possible), si toute réalisation égalitaire de $\mathscr{L}$ qui satisfait $\mathscr{A}$ satisfait aussi F. Une formule F de $\mathscr{L}$ est appelée théorème égalitaire de $\mathscr{L}$ si sa clôture est satisfaite par toutes les réalisations égalitaires de $\mathscr{L}$.

Désignons par $\mathscr{E}_{\mathscr{L}}$ l'ensemble des formules suivantes de $\mathscr{L}$ qu'on appelle axiomes d'égalité pour $\mathscr{L}$:

1° $\mathsf{\Lambda}x^{(i)} (x^{(i)} = x^{(i)})$ pour chaque entier $i (1 \leqslant i \leqslant k)$, où $x^{(i)}$ est une variable de type i.

$$2^{\circ}\ \wedge x_1^{(i_1)} \dots \wedge x_n^{(i_n)} \wedge y_1^{(j_1)} \dots \wedge y_n^{(j_n)}[x_1^{(i_1)} = y_1^{(j_1)} \wedge \dots \wedge x_n^{(i_n)} = y_n^{(j_n)} \wedge Rx_1^{(i_1)} \dots x_n^{(i_n)} \to Ry_1^{(j_1)} \dots y_n^{(j_n)}]$$

pour chaque symbole relationnel $R \in \mathrm{R}_{\mathscr{L}}^{(n)}$ (y compris E lorsque $n = 2$), et pour chaque suite $i_1, \dots, i_n, j_1, \dots, j_n$ de $2\,n$ entiers compris entre 1 et k ; $x_1^{(i_1)}, \dots, x_n^{(i_n)}, y_1^{(j_1)}, \dots, y_n^{(j_n)}$ sont des variables de types respectifs $i_1, \dots, i_n, j_1, \dots, j_n$.

$$3^{\circ}\ \wedge x_1^{(i_1)} \dots \wedge x_n^{(i_n)} \wedge y_1^{(i_1)} \dots \wedge y_n^{(i_n)}[x_1^{(i_1)} = y_1^{(i_1)} \wedge \dots \wedge x_n^{(i_n)} = y_n^{(i_n)} \wedge Sx_1^{(i_1)} \dots x_n^{(i_n)} \to Sy_1^{(i_1)} \dots y_n^{(i_n)}]$$

pour chaque symbole relationnel S de type $(i_1, \dots, i_n)$; $x_j^{(i)}$ et $y_j^{(i)}$ sont des variables de type i.

Soit $\mathfrak{M}$ un modèle de $\mathscr{E}_{\mathscr{L}}$, d'ensembles de base $U_1, \dots, U_k$. La valeur $\overline{E}_{\mathfrak{M}}$ du symbole relationnel E dans ce modèle est le graphe d'une relation d'équivalence sur $U_1 \cup \dots \cup U_k$: en effet $\mathscr{E}_{\mathscr{L}}$ contient les formules :

$$\wedge x_1^{(i_1)} \wedge x_2^{(i_2)} \wedge y_1^{(j_1)} \wedge y_2^{(j_2)}[x_1^{(i_1)} = y_1^{(j_1)} \wedge x_2^{(i_2)} = y_2^{(j_2)} \wedge x_1^{(i_1)} = x_2^{(i_2)} \to y_1^{(j_1)} = y_2^{(j_2)}]$$

donc $\mathfrak{M}$ satisfait ces formules.

On déduit alors de $\mathfrak{M}$ une réalisation égalitaire $\mathfrak{M}'$ de $\mathscr{L}$ de la façon suivante : les ensembles de base de $\mathfrak{M}'$ sont les images de $U_1, \dots, U_k$ dans l'application canonique de $U_1 \cup \dots \cup U_k$ sur $U_1 \cup \dots \cup U_k/\overline{E}_{\mathfrak{M}}$. Si c est un symbole de constante de $\mathscr{L}$, soit $\overline{c}_{\mathfrak{M}}$ la valeur qu'il prend dans $\mathfrak{M}$; alors sa valeur $\overline{c}_{\mathfrak{M}'}$ dans $\mathfrak{M}'$ est la classe d'équivalence de $\overline{c}_{\mathfrak{M}}$ pour la relation d'équivalence $\overline{E}_{\mathfrak{M}}$.

Si R est un symbole relationnel de $\mathscr{L}$ (à n variables ou de type $(i_1, \dots, i_n)$) dont la valeur dans $\mathfrak{M}$ est $\overline{R}_{\mathfrak{M}}$, on définit sa valeur $\overline{R}_{\mathfrak{M}'}$ dans $\mathfrak{M}'$ comme l'image de $\overline{R}_{\mathfrak{M}}$ par l'application canonique de $U_1 \cup \dots \cup U_k$ sur $U_1 \cup \dots \cup U_k/\overline{E}_{\mathfrak{M}}$.

De la même façon qu'au chapitre 3, on montre que pour chaque formule A de $\mathscr{L}$, qui prend respectivement les valeurs $\overline{A}_{\mathfrak{M}}$ et $\overline{A}_{\mathfrak{M}'}$ dans $\mathfrak{M}$ et $\mathfrak{M}'$, $\overline{A}_{\mathfrak{M}}$ est saturée pour la relation d'équivalence $\overline{E}_{\mathfrak{M}}$, et $\overline{A}_{\mathfrak{M}'}$ est l'image de $\overline{A}_{\mathfrak{M}}$ par l'application canonique de $U_1 \cup \dots \cup U_k$ sur $U_1 \cup \dots \cup U_k/\overline{E}_{\mathfrak{M}}$.

En particulier si A est une formule close de $\mathscr{L}$, elle est simultanément satisfaite ou non satisfaite par $\mathfrak{M}$ et $\mathfrak{M}'$.

PROPOSITION 3. — *Pour qu'une formule close F de $\mathscr{L}$ soit conséquence égalitaire d'un ensemble $\mathscr{A}$ de formules closes de $\mathscr{L}$, il faut et il suffit que F soit conséquence de $(\mathscr{A}, \mathscr{E}_{\mathscr{L}})$.*

En effet si F est conséquence de $(\mathscr{A}, \mathscr{E}_{\mathscr{L}})$, tout modèle égalitaire de $\mathscr{A}$ satisfait $\mathscr{E}_{\mathscr{L}}$, donc satisfait F. Si F n'est pas conséquence de $(\mathscr{A}, \mathscr{E}_{\mathscr{L}})$, il existe un modèle $\mathfrak{M}$ de $(\mathscr{A}, \mathscr{E}_{\mathscr{L}})$ qui satisfait $\neg F$. Alors $\mathfrak{M}'$ est un modèle égalitaire de $\mathscr{A}$ qui satisfait $\neg F$, ce qui montre que F n'est pas conséquence égalitaire de $\mathscr{A}$.

C. q. f. d.

Le théorème de finitude pour le calcul des prédicats à k types d'objets avec égalité se déduit du théorème de finitude pour le calcul des prédicats sans égalité (théorème 1) de la même façon qu'au chapitre 3. Il s'énonce :

THÉORÈME 3. — *Soit $\mathscr{A}$ un ensemble de formules closes du langage égalitaire $\mathscr{L}$, dont tout sous-ensemble fini a un modèle égalitaire. Alors $\mathscr{A}$ a un modèle égalitaire.*

Le théorème d'interpolation pour le calcul des prédicats avec égalité s'énonce :

THÉORÈME 4. — *Soient F, G deux formules closes du langage égalitaire $\mathscr{L}$, telles que $F \wedge G$ n'ait pas de modèle égalitaire. Alors il existe une formule close H de $\mathscr{L}$, dont les symboles relationnels (l'égalité mise à part) et les types sont communs à F et G, et telle que $F \to H$ et $G \to \neg H$ soient des théorèmes égalitaires.*

On prend pour $\mathscr{L}$ le langage de $F \wedge G$; soient $\mathscr{L}_1$ le langage formé des symboles et des types qui sont dans F sans être dans G, $\mathscr{L}_2$ le langage formé des symboles et des types communs à F et à G, $\mathscr{L}_3$ le langage formé de symboles et des types qui sont dans G sans être dans F.

Il suffit de montrer que $(F, G, \mathscr{E}_{\mathscr{L}_1 \cup \mathscr{L}_2}, \mathscr{E}_{\mathscr{L}_2 \cup \mathscr{L}_3})$ n'a pas de modèle ; car, en appliquant le théorème d'interpolation aux formules $\mathscr{E}_{\mathscr{L}_1 \cup \mathscr{L}_2} \wedge F$, $\mathscr{E}_{\mathscr{L}_2 \cup \mathscr{L}_3} \wedge G$, on obtient une formule H de $\mathscr{L}_2$, telle que

$$\mathscr{E}_{\mathscr{L}_1 \cup \mathscr{L}_2}, F \vdash H \qquad \text{et} \qquad \mathscr{E}_{\mathscr{L}_2 \cup \mathscr{L}_3}, G \vdash \neg H ;$$

par suite $F \to H$ et $G \to \neg H$ sont des théorèmes égalitaires.

Soit alors $\mathfrak{M}$ un modèle de

$$(F, G, \mathscr{E}_{\mathscr{L}_1 \cup \mathscr{L}_2}, \mathscr{E}_{\mathscr{L}_2 \cup \mathscr{L}_3}) ;$$

désignons par V_1 (resp. V_2, V_3) la réunion des ensembles de base de $\mathfrak{M}$ dont le type est dans $\mathscr{L}_1$ (resp. $\mathscr{L}_2$, $\mathscr{L}_3$). On définit un modèle $\mathfrak{M}_1$ de

$$(F, G, \mathscr{E}_{\mathscr{L}_1 \cup \mathscr{L}_2}, \mathscr{E}_{\mathscr{L}_2 \cup \mathscr{L}_3})$$

qui a les mêmes ensembles de base que $\mathfrak{M}$, de la façon suivante : soit R un symbole relationnel à n variables de $\mathscr{L}(R \in \mathrm{R}_{\mathscr{L}}^{(n)})$ qui prend la valeur $\overline{R}_{\mathfrak{M}}$ dans $\mathfrak{M}$; alors sa valeur $\overline{R}_{\mathfrak{M}_1}$ dans $\mathfrak{M}_1$ est par définition :

$$\overline{R}_{\mathfrak{M}_1} = \{ (u_1, u_2, ..., u_n) \in (V_1 \cup V_2 \cup V_3)^n \} ;$$

$(u_1, ..., u_n) \in \overline{R}_{\mathfrak{M}}$ et $u_1, ..., u_n$ sont tous éléments de $V_1 \cup V_2$ ou tous éléments de $V_2 \cup V_3 \}$.

Si S est un symbole relationnel de $\mathscr{L}$ de type $(i_1, ..., i_n)$ qui prend la valeur $\overline{S}_{\mathfrak{M}}$ dans $\mathfrak{M}$, on pose $\overline{S}_{\mathfrak{M}_1} = \overline{S}_{\mathfrak{M}}$. (Remarquons que les types $i_1, ..., i_n$ de S appartiennent tous à $\mathscr{L}_1 \cup \mathscr{L}_2$ si S apparaît dans F, ou à $\mathscr{L}_2 \cup \mathscr{L}_3$ si S apparaît dans G ; donc si $(u_1, ..., u_n) \in \overline{S}_{\mathfrak{M}}$, $u_1, ..., u_n$ sont tous éléments de $V_1 \cup V_2$ ou tous éléments de $V_2 \cup V_3$).

Il est clair que $\mathfrak{M}$ et $\mathfrak{M}_1$ satisfont les mêmes formules de $\mathscr{L}_1 \cup \mathscr{L}_2$ et de $\mathscr{L}_2 \cup \mathscr{L}_3$. Donc $\mathfrak{M}_1$ est un modèle de

$$(F , G , \mathscr{E}_{\mathscr{L}_1 \cup \mathscr{L}_2} , \mathscr{E}_{\mathscr{L}_2 \cup \mathscr{L}_3}) .$$

On définit une relation d'équivalence $\tilde{E}$ sur $V = V_1 \cup V_2 \cup V_3$ de la façon suivante :

$$(x, y) \in \tilde{E} \Leftrightarrow ((x, y) \in \overline{E}_{\mathfrak{M}_1})$$

$$\text{ou} \qquad (x \in V_1 , \ y \in V_3 \quad \text{et} \quad \exists z \in V_2 , \ (x, z) \in \overline{E}_{\mathfrak{M}_1} \quad \text{et} \quad (y, z) \in \overline{E}_{\mathfrak{M}_1})$$

$$\text{ou} \qquad (x \in V_3 , \ y \in V_1 \quad \text{et} \quad \exists z \in V_2 , \ (x, z) \in \overline{E}_{\mathfrak{M}_1} \quad \text{et} \quad (y, z) \in \overline{E}_{\mathfrak{M}_1}) .$$

Il est clair que $\tilde{E}$ est réflexive et symétrique ; de plus c'est une relation d'équivalence sur $V_1 \cup V_2$ et $V_2 \cup V_3$: car sur ces ensembles elle est identique à $\overline{E}_{\mathfrak{M}_1}$, qui est une relation d'équivalence sur $V_1 \cup V_2$ puisque $\mathfrak{M}_1$ satisfait $\mathscr{E}_{\mathscr{L}_1 \cup \mathscr{L}_2}$, et sur $V_2 \cup V_3$ puisque $\mathfrak{M}_1$ satisfait $\mathscr{E}_{\mathscr{L}_2 \cup \mathscr{L}_3}$. Si $(x, y) \in \tilde{E}$ et $(y, z) \in \tilde{E}$ et si, par exemple, $x \in V_1, y \in V_3, z \in V_1$, il existe $u, v \in V_2$ tels que $(x, u), (u, y), (v, y), (z, v)$ soient éléments de $\overline{E}_{\mathfrak{M}_1}$. Comme $\overline{E}_{\mathfrak{M}_1}$ est une relation d'équivalence sur $V_2 \cup V_3$ on a $(u, v) \in \overline{E}_{\mathfrak{M}_1}$, et donc $(x, z) \in \overline{E}_{\mathfrak{M}_1}$, d'où $(x, z) \in \tilde{E}$ puisque $x, z \in V_1$. $\tilde{E}$ est donc bien une relation d'équivalence sur V.

Pour chaque symbole relationnel R à n variables ($R \in \mathrm{R}_{\mathscr{L}}^{(n)}$) on définit :

$$\tilde{R} = \{ (u_1, ..., u_n) \in V^n ;$$

il existe $(v_1, ..., v_n) \in V^n$, avec $(u_1, v_1) \in \tilde{E}, ..., (u_n, v_n) \in \tilde{E}$ et $(v_1, ..., v_n) \in \overline{R}_{\mathfrak{M}_1} \}$.
Pour chaque symbole relationnel S de type $(i_1, ..., i_n)$ on pose

$$\tilde{S} = \overline{S}_{\mathfrak{M}_1} = \overline{S}_{\mathfrak{M}} .$$

$\tilde{E}$, les $\tilde{R}$ et les $\tilde{S}$ définissent une réalisation $\tilde{\mathfrak{M}}$ de $\mathscr{L}$ qui a les mêmes ensembles de base que $\mathfrak{M}$ et $\mathfrak{M}_1$.

$\tilde{\mathfrak{M}}$ *satisfait* $\mathscr{E}_{\mathscr{L}}$: supposons que $(u_1, ..., u_n) \in \tilde{R}$ (où $R \in \mathrm{R}_{\mathscr{L}}^{(n)}$) et que

$$(u_1, v_1) \in \tilde{E}, ..., (u_n, v_n) \in \tilde{E} ;$$

alors, par définition de $\tilde{R}$, il existe $(u'_1, ..., u'_n) \in \overline{R}_{\mathfrak{M}_1}$, avec

$$(u_1, u'_1) \in \tilde{E}, ..., (u_n, u'_n) \in \tilde{E} ; \quad \text{donc} \quad (u'_1, v_1) \in \tilde{E}, ..., (u'_n, v_n) \in \tilde{E}$$

et donc, par définition de $\tilde{R}$, $(v_1, ..., v_n) \in \tilde{R}$. Cela montre que les axiomes d'égalité correspondant au symbole relationnel R sont satisfaits dans $\tilde{\mathfrak{M}}$.

D'autre part si S est un symbole relationnel de type $(i_1, ..., i_n)$ de $\mathscr{L}$, S apparaît dans F par exemple. Les types $i_1, ..., i_n$ de S sont alors contenus dans

$\mathscr{L}_1 \cup \mathscr{L}_2$. Donc l'axiome d'égalité pour S est satisfait par $\mathfrak{M}_1$ ($\mathfrak{M}_1$ satisfait $\mathscr{E}_{\mathscr{L}_1 \cup \mathscr{L}_2}$) donc par $\widetilde{\mathfrak{M}}$ puisque $\widetilde{S} = \overline{S}_{\mathfrak{M}_1}$.

Si $R \in \mathrm{R}_{\mathscr{L}}^{(n)}$ *et si* $u_1, ..., u_n \in V_1 \cup V_2$ *(resp.* $V_2 \cup V_3$*) alors*

$$(u_1, ..., u_n) \in \widetilde{R} \Leftrightarrow (u_1, ..., u_n) \in \overline{R_{\mathfrak{M}_1}} .$$

En effet si $(u_1, ..., u_n) \in \overline{R}_{\mathfrak{M}_1}$, alors $(u_1, ..., u_n) \in \widetilde{R}$; inversement, si $(u_1, ..., u_n) \in \widetilde{R}$ et si $u_1, ..., u_n \in V_1 \cup V_2$, il existe $v_1, ..., v_n$ tels que

$$(u_1, v_1) \in \widetilde{E}, ..., (u_n, v_n) \in \widetilde{E} \qquad \text{et} \qquad (v_1, ..., v_n) \in \overline{R_{\mathfrak{M}_1}} .$$

D'où il résulte que

$$v_1, ..., v_n \in V_1 \cup V_2 \qquad \text{ou} \qquad v_1, ..., v_n \in V_2 \cup V_3 .$$

Si $v_1, ..., v_n \in V_1 \cup V_2$, comme $(u_i, v_i) \in \widetilde{E}$, on a $(u_i, v_i) \in \overline{E}_{\mathfrak{M}_1}$; puisque $\mathfrak{M}_1$ satisfait $\mathscr{E}_{\mathscr{L}_1 \cup \mathscr{L}_2}$, on a alors $(u_1, ..., u_n) \in \overline{R}_{\mathfrak{M}_1}$. Supposons alors

$$v_1, ..., v_n \in V_2 \cup V_3 ;$$

si $v_i \in V_3$, comme $(u_i, v_i) \in \widetilde{E}$ il existe $w_i \in V_2$ (avec peut-être $w_i = u_i$) tel que $(u_i, w_i) \in \overline{E}_{\mathfrak{M}_1}$ et $(w_i, v_i) \in \overline{E}_{\mathfrak{M}_1}$; si $v_i \in V_2$ on prend $w_i = v_i$ et on a les mêmes relations. Comme $\mathfrak{M}_1$ satisfait $\mathscr{E}_{\mathscr{L}_2 \cup \mathscr{L}_3}$, et que $(v_1, ..., v_n) \in \overline{R}_{\mathfrak{M}_1}$, on a

$$(w_1, ..., w_n) \in \overline{R}_{\mathfrak{M}_1} ;$$

comme $\mathfrak{M}_1$ satisfait $\mathscr{E}_{\mathscr{L}_1 \cup \mathscr{L}_2}$ on en déduit $(u_1, ..., u_n) \in \overline{R}_{\mathfrak{M}_1}$. Cela démontre le résultat annoncé.

Il en résulte que $\widetilde{\mathfrak{M}}$ et $\mathfrak{M}_1$ satisfont les mêmes formules de $\mathscr{L}_1 \cup \mathscr{L}_2$ et de $\mathscr{L}_2 \cup \mathscr{L}_3$. Donc $\widetilde{\mathfrak{M}}$ satisfait F, G. Comme $\widetilde{\mathfrak{M}}$ satisfait $\mathscr{E}_{\mathscr{L}}$, $(F, G, \mathscr{E}_{\mathscr{L}})$ a un modèle, donc (proposition 3) $F \wedge G$ a un modèle égalitaire, contrairement à l'hypothèse. C. q. f. d.

Langages égalitaires à k types d'objets avec symboles fonctionnels.

Nous nous bornerons dans ce paragraphe à donner les définitions et à énoncer les théorèmes. Les démonstrations sont faites dans l'exercice 1.

Un langage égalitaire $\mathscr{L}$, à k types d'objets avec symboles fonctionnels est par définition constitué par :

1° k ensembles infinis disjoints $V_{\mathscr{L}}^{(1)}, ..., V_{\mathscr{L}}^{(k)}$; $V_{\mathscr{L}}^{(i)}$ $(1 \leqslant i \leqslant k)$ est l'ensemble des variables de type i de $\mathscr{L}$.

2° Pour chaque entier $n \geqslant 0$, un ensemble $\mathrm{R}_{\mathscr{L}}^{(n)}$, dont les éléments sont appelés symboles relationnels à n variables (de type quelconque). De plus on sup-

pose que $R^{(2)}_{\mathscr{L}} \neq \phi$ et qu'on a distingué un élément E de $R^{(2)}_{\mathscr{L}}$ appelé symbole d'égalité.

3° Pour chaque suite $(i_1, ..., i_n)$ formée d'entiers compris entre 1 et k, un ensemble $S^{(i_1,...,i_n)}_{\mathscr{L}}$ dont les éléments sont appelés symboles relationnels de type $(i_1, ..., i_n)$ (ou symboles relationnels à n variables dont la première est de type i_1, ..., la n-ième de type i_n).

4° Pour chaque suite $(i, i_1, ..., i_n)$ formée d'entiers compris entre 1 et k, un ensemble $F^{(i,i_1,...,i_n)}_{\mathscr{L}}$ dont les éléments sont appelés symboles fonctionnels de type $(i, i_1, ..., i_n)$ (ou symboles fonctionnels à n variables, la première de type i_1, ..., la n-ième de type i_n, à valeurs de type i).

Tous ces ensembles sont supposés disjoints deux à deux.

On définit (voir exercice 1) l'ensemble T des termes de $\mathscr{L}$, qui se partage en k ensembles disjoints $T^{(1)}, ..., T^{(k)}$; $T^{(i)}$ $(1 \leqslant i \leqslant k)$ est l'ensemble des termes de type i de $\mathscr{L}$.

Les formules atomiques de $\mathscr{L}$ sont de l'une des deux formes suivantes :

$Rt_1 ... t_n$, où $R \in R^{(n)}_{\mathscr{L}}$ et $t_1, ..., t_n$ sont des termes de types quelconques ; en particulier la formule atomique $Et_1\, t_2$ sera notée $t_1 = t_2$.

$St^{(i_1)}_1 ... t^{(i_n)}_n$, où S est un symbole relationnel de type $(i_1, ..., i_n)$ et où $t^{(i_1)}_1, ..., t^{(i_n)}_n$ sont des termes de types respectifs $i_1, ..., i_n$.

L'ensemble des formules de $\mathscr{L}$ est alors l'ensemble des schémas fonctionnels construits avec les formules atomiques comme symboles à 0 variable, $\neg$ et $\forall x$ (pour chaque $x \in V^{(1)}_{\mathscr{L}} \cup \cdots \cup V^{(k)}_{\mathscr{L}}$) comme symboles à 1 variable, $\vee$ comme symbole à 2 variables.

Une réalisation égalitaire de $\mathscr{L}$ est par définition constituée par :

1) k ensembles non vides $U_1, ..., U_k$; $U_i (1 \leqslant i \leqslant k)$ est appelé l'ensemble de base de type i de la réalisation.

2° Pour chaque entier $n \geqslant 0$ une application $R \to \overline{R}$ de $R^{(n)}_{\mathscr{L}}$ dans

$$\mathfrak{P}[(U_1 \cup \cdots \cup U_k)^n].$$

On suppose de plus que $\overline{E}$ est la relation d'égalité sur $U_1 \cup \cdots \cup U_k$, c'est-à-dire l'ensemble des couples (u, u) pour $u \in U_1 \cup \cdots \cup U_k$.

3° Pour chaque suite $(i_1, ..., i_n)$ d'entiers compris entre 1 et k une application $S \mapsto \overline{S}$ de $S^{(i_1,...,i_n)}_{\mathscr{L}}$ dans $\mathfrak{P}(U_{i_1} \times \cdots \times U_{i_n})$.

4° Pour chaque suite $(i, i_1, ..., i_n)$ d'entiers compris entre 1 et k, une application $f \to \bar{f}$ de $F^{(i,i_1,...,i_n)}_{\mathscr{L}}$ dans l'ensemble des applications de $U_{i_1} \times \cdots \times U_{i_n}$ dans U_i.

Soit δ un élément de $U_1^{V^{(1)}_{\mathscr{L}}} \times \cdots \times U_k^{V^{(k)}_{\mathscr{L}}}$, c'est-à-dire une application de

$V_{\mathscr{L}}^{(1)} \cup \cdots \cup V_{\mathscr{L}}^{(k)}$ dans $U_1 \cup \cdots \cup U_k$ telle que $\delta(V_{\mathscr{L}}^{(i)}) \subset U_i$ pour chaque i $(1 \leqslant i \leqslant k)$.

Alors δ se prolonge d'une façon naturelle en une application, notée aussi δ, de T dans $U_1 \cup \cdots \cup U_k$, telle que $\delta(T^{(i)}) \subset U_i$ pour chaque i $(1 \leqslant i \leqslant k)$ (voir exercice 1).

La valeur $\overline{F}$ prise par une formule F de $\mathscr{L}$ dans la réalisation considérée est un sous-ensemble de $U_1^{V_{\mathscr{L}}^{(1)}} \times \cdots \times U_k^{V_{\mathscr{L}}^{(k)}}$, qu'on définit par récurrence sur la longueur de F de la façon suivante :

a) Si F est une formule atomique, elle s'écrit $Rt_1 \ldots t_n$ avec $R \in \mathrm{R}_{\mathscr{L}}^{(n)}$ ou $R \in \mathrm{S}_{\mathscr{L}}^{(i_1, \ldots, i_n)}$; la valeur $\overline{F}$ prise par F est alors l'ensemble des

$$\delta \in U_1^{V_{\mathscr{L}}^{(1)}} \times \cdots \times U_k^{V_{\mathscr{L}}^{(k)}} \quad \text{telles que} \quad (\delta(t_1), \ldots, \delta(t_n)) \in \overline{R}.$$

b) $\overline{F \vee G} = \overline{F} \cup \overline{G}$; $\overline{\neg F} = \complement \overline{F}$;
$\overline{\forall x F}$ = projection de $\overline{F}$ suivant la variable x (c'est l'ensemble des

$$\delta \in U_1^{V_{\mathscr{L}}^{(1)}} \times \cdots \times U_k^{V_{\mathscr{L}}^{(k)}}$$

telles qu'il existe $\delta_1 \in \overline{F}$, δ_1 étant égale à δ pour toute variable de $\mathscr{L}$ sauf peut-être x).

On définit alors les énoncés : « la formule close F est satisfaite par la réalisation $\mathfrak{M}$ » et « la formule close F est conséquence de l'ensemble de formules closes $\mathscr{A}$ » de la même façon qu'au début de ce chapitre.

Le théorème de finitude, sous la forme énoncée au théorème 3, reste vrai pour les langages avec symboles fonctionnels. Le théorème d'interpolation s'énonce :

THÉORÈME 5. — *Soient F, G deux formules closes du langage égalitaire $\mathscr{L}$ à k types d'objets avec symboles fonctionnels. Si $F \wedge G$ n'a pas de modèle égalitaire, il existe une formule close H de $\mathscr{L}$, dont les symboles relationnels (l'égalité mise à part), les symboles fonctionnels et les types, sont communs à F et G, et telle que $F \to H$ et $G \to \neg H$ soient des théorèmes égalitaires.*

Les démonstrations sont données dans l'exercice 1.

Théorie des types. Calcul des prédicats d'ordre fini.

Soit $\mathbf{T}$ le plus petit ensemble ayant les propriétés suivantes :

1° $0 \in \mathbf{T}$.

2° Si $\tau_1, \tau_2, \ldots, \tau_n$ sont des éléments de $\mathbf{T}$, la suite ordonnée $(\tau_1, \ldots, \tau_n)$ est un élément de $\mathbf{T}$.

Les éléments de $\mathbf{T}$ sont appelés types. Si τ est un type $\neq 0$, il existe des types $\tau_1, \ldots, \tau_n$ tels que $\tau = (\tau_1, \ldots, \tau_n)$ (puisque l'ensemble des types qui ont cette propriété satisfait les conditions 1 et 2 ci-dessus). L'entier n, et les types $\tau_1, \ldots, \tau_n$ sont évidemment déterminés de façon unique par le type τ.

Etant donné un type $\tau \neq 0$ il existe un entier $N \geqslant 0$ ayant la propriété suivante : toute suite $\tau_1, ..., \tau_k$ de types $\neq 0$ telle que $\tau_k = \tau$, et telle que pour tout $i (1 \leqslant i \leqslant k - 1)$, τ_i soit un des éléments de la suite constituant τ_{i+1}, a une longueur $k \leqslant N$ (l'ensemble des types pour lesquels il existe un tel entier satisfait les conditions 1 et 2 ci-dessus). *Nous appellerons rang de τ le plus petit de ces entiers N* : c'est la longueur de la plus longue des suites $\tau_1, \tau_2, ..., \tau_k$ de types $\neq 0$ tels que $\tau_k = \tau$, et pour tout i $(1 \leqslant i \leqslant k - 1)$ τ_i soit un des éléments de la suite constituant τ_{i+1}.

Soit $r(\tau)$ le rang du type $\tau \neq 0$. On pose $r(0) = 0$. On a immédiatement l'égalité :

$$r(\tau) = 1 + \sup\left[r(\tau_1), ..., r(\tau_n)\right] \quad \text{pour } \tau = (\tau_1, ..., \tau_n) .$$

Etant donné un type τ, on appelle *clôture transitive de τ et on désigne par* $[\tau]$ le plus petit ensemble ayant les propriétés suivantes :

1′ $\tau \in [\tau]$.

2′ Si $\tau' = (\tau_1, ..., \tau_n) \in [\tau]$, alors $\tau_1, ..., \tau_n$ sont des éléments de $[\tau]$.

Il résulte de cette définition que *si* $\tau = (\tau_1, ..., \tau_n)$, on a

$$[\tau] = \{\tau\} \cup [\tau_1] \cup \cdots \cup [\tau_n] ;$$

en effet $[\tau]$ a les deux propriétés définissant $[\tau_i]$, donc $[\tau] \supset [\tau_i]$ et par suite :

$$[\tau] \supset \{\tau\} \cup [\tau_1] \cup \cdots \cup [\tau_n] .$$

Mais inversement $\{\tau\} \cup [\tau_1] \cup \cdots \cup [\tau_n]$ a les deux propriétés définissant $[\tau]$, donc le contient. Par suite $[\tau]$ *est un sous-ensemble fini de* **T** : d'après la propriété précédente, l'ensemble des types τ tels que $[\tau]$ soit un sous-ensemble fini de **T** a les deux propriétés définissant **T**, donc est identique à **T**.

Tous les éléments de $[\tau]$ *différents de τ ont un rang strictement inférieur à celui de τ.*

Démonstration immédiate par récurrence sur le rang de τ.

On définit sur **T** *une relation d'ordre en posant $\tau \leqslant \sigma$ si et seulement si $\tau \in [\sigma]$.*

On a évidemment $\tau \leqslant \tau$. Si $\tau \leqslant \sigma$ et $\sigma \leqslant \tau$ les rangs de τ et σ sont égaux. Comme $\tau \in [\sigma]$ on a $\tau = \sigma$. Si $\sigma \leqslant \tau$ et $\tau \leqslant \upsilon$ on a $\sigma \in [\upsilon]$: démonstration immédiate par récurrence sur le rang de υ.

On considère un langage égalitaire $\mathscr{L}$ (au sens du chapitre 2, c'est-à-dire à un seul type d'objets) et on se donne deux familles d'ensembles (V^τ) et (ε_τ) où τ décrit l'ensemble des types non nuls ; les ensembles V^τ sont supposés infinis, disjoints deux à deux, et disjoints de $\mathscr{L}$. Les ε_τ sont supposés distincts, et non éléments de $\mathscr{L} \cup \bigcup_{\tau \neq 0} V^\tau$. L'ensemble des variables de $\mathscr{L}$ sera désigné par V^0.

Pour chaque type τ, nous désignerons par $\mathscr{L}^\tau$ le langage égalitaire à plusieurs types d'objets avec symboles fonctionnels défini de la façon suivante :

— Les divers types d'objets de $\mathscr{L}^\tau$ sont les types σ, $\sigma \leqslant \tau$. L'ensemble des variables de type σ est V^σ.

— Les symboles fonctionnels de $\mathscr{L}^\tau$ sont les symboles fonctionnels de $\mathscr{L}$, considérés comme étant à variables et valeur de type 0.

— Les symboles relationnels de $\mathscr{L}^\tau$ sont :

1° Les symboles relationnels de $\mathscr{L}$, sauf le symbole d'égalité, considérés comme ayant toutes leurs variables de type 0 ; le symbole d'égalité de $\mathscr{L}^\tau$ est celui de $\mathscr{L}$.

2° Les ε_σ pour $\sigma \neq 0$, $\sigma \leqslant \tau$; si $\sigma = (\sigma_1, ..., \sigma_n)$, ε_σ est un symbole à $n+1$ variables, la première de type σ_1, la seconde de type σ_2, ..., la n-ième de type σ_n, la $(n+1)$-ième de type σ.

Les variables de types σ (c'est-à-dire les éléments de V^σ) seront écrites avec σ en exposant (x^σ, y^σ, ...).

Le type 0 est appelé aussi type des individus ; on dira par exemple variable d'individu pour variable de type 0. Le type (0, 0, ..., 0) (suite de n zéros) est aussi appelé type des relations n-adiques (monadiques pour $n = 1$, dyadiques pour $n = 2$). Le type (0) est encore appelé type des ensembles d'individus, le type ((0)) type des ensembles d'ensembles d'individus, etc.

Si $\sigma = (\sigma_1, ..., \sigma_n)$ est un type $\leqslant \tau$ la formule $\varepsilon_\sigma\, x_1^{\sigma_1}\, x_2^{\sigma_2} \dots x_n^{\sigma_n}\, x^\sigma$ qui est une formule atomique de $\mathscr{L}^\tau$ sera aussi écrite dans la suite : $(x_1^{\sigma_1}, ..., x_n^{\sigma_n})\ \varepsilon_\sigma\ x^\sigma$ ou encore $(x_1^{\sigma_1}, ..., x_n^{\sigma_n})\ \varepsilon\ x^\sigma$.

Le langage $\mathscr{L}^\tau$ est désigné sous le nom de *langage d'ordre τ construit sur $\mathscr{L}$*. Les formules de $\mathscr{L}^\tau$ sont appelées formules d'ordre τ de $\mathscr{L}$. Il est clair que si $\tau \leqslant \tau'$, on a $\mathscr{L}^\tau \subset \mathscr{L}^{\tau'}$; donc toute formule d'ordre τ est aussi une formule d'ordre τ'. Les formules d'ordre 0 de $\mathscr{L}$ sont les formules ordinaires de $\mathscr{L}$.

Pour chaque type τ nous désignerons par $\mathscr{X}_\tau$ l'ensemble des formules d'ordre τ suivantes :

$$\wedge x^\alpha \wedge x^\beta (x^\alpha \neq x^\beta) \qquad (\text{pour} \quad \alpha, \beta \leqslant \tau\ ; \quad \alpha \neq \beta)$$

$$\wedge x^\alpha \wedge y^\alpha [\wedge x_1^{\alpha_1} \wedge x_2^{\alpha_2} \dots \wedge x_n^{\alpha_n} [(x_1^{\alpha_1}, ..., x_n^{\alpha_n})\ \varepsilon\ x^\alpha \leftrightarrow (x_1^{\alpha_1}, ..., x_n^{\alpha_n})\ \varepsilon\ y^\alpha] \rightarrow x^\alpha = y^\alpha]$$

(pour chaque type $\alpha \leqslant \tau$ avec $\alpha = (\alpha_1, ..., \alpha_n)$). (Cette formule est appelée axiome d'extensionnalité d'ordre α).

Une réalisation d'ordre τ de $\mathscr{L}$ ou encore *τ-réalisation* est par définition une réalisation égalitaire de $\mathscr{L}^\tau$ satisfaisant $\mathscr{X}_\tau$. Une réalisation d'ordre 0 de $\mathscr{L}$ est donc une réalisation de $\mathscr{L}$ au sens ordinaire. Les ensembles de base E_σ ($\sigma \leqslant \tau$) d'une réalisation d'ordre τ de $\mathscr{L}$ sont donc disjoints. Si $\sigma = (\sigma_1, ..., \sigma_n)$ et si $a \in E_\sigma$, un élément $(a_1, ..., a_n)$ de $E_{\sigma_1} \times \cdots \times E_{\sigma_n}$, tel que $(a_1, ..., a_n, a) \in \bar{\varepsilon}_\sigma$ (valeur de ε_σ dans la réalisation considérée) sera appelé « élément » de a dans cette réalisation. D'après les axiomes d'extensionnalité, deux éléments a, b de E_σ qui ont les mêmes « éléments » sont identiques.

Soit $\mathfrak{M}_\tau$ une réalisation d'ordre τ de $\mathscr{L}$ (c'est-à-dire un modèle de $\mathscr{X}_\tau$),

d'ensembles de base E_σ ($\sigma \leqslant \tau$). Il est clair que si $\tau' \leqslant \tau$ la restriction de $\mathfrak{M}^\tau$ au langage $\mathscr{L}^{\tau'}$ et aux ensembles de base E_σ ($\sigma \leqslant \tau'$) est un modèle de $\mathscr{L}_{\tau'}$, c'est-à-dire une réalisation $\mathfrak{M}^{\tau'}$ d'ordre τ' de $\mathscr{L}$. $\mathfrak{M}^{\tau'}$ est appelé réalisation d'ordre τ' induite par $\mathfrak{M}^\tau$, et $\mathfrak{M}^\tau$ est dite construite sur $\mathfrak{M}^{\tau'}$. En particulier pour $\tau' = 0$, on voit que chaque réalisation d'ordre τ induit une réalisation ordinaire de $\mathscr{L}$ sur laquelle elle est construite.

THÉORÈME. — *Soit $\mathfrak{M}$ une réalisation (d'ordre 0) de $\mathscr{L}$. Il existe une réalisation $\mathfrak{M}^\tau$ d'ordre τ de $\mathscr{L}$, et une seule à un isomorphisme près ayant les propriétés suivantes* :

1° *$\mathfrak{M}^\tau$ est construite sur $\mathfrak{M}$.*

2° *Toute réalisation $\mathfrak{N}^\tau$ d'ordre τ de $\mathscr{L}$ construite sur $\mathfrak{M}$ se plonge dans $\mathfrak{M}^\tau$ en conservant chaque élément de $\mathfrak{M}$.*

$\mathfrak{M}^\tau$ est appelée réalisation principale d'ordre τ construite sur $\mathfrak{M}$.

Soit E_0 l'ensemble de base de $\mathfrak{M}$. On définit E_σ ensemble de base de type σ de $\mathfrak{M}^\tau$, par récurrence sur le rang de σ, de la façon suivante : si $\sigma = (\sigma_1, ..., \sigma_n)$, E_σ est un ensemble disjoint de tous les E_α déjà définis, et tels que

$$\operatorname{card}(E_\sigma) = 2^{\operatorname{card}(E_{\sigma_1} \times \cdots \times E_{\sigma_n})}.$$

Il existe donc une bijection φ_σ de E_σ sur $\mathfrak{P}(E_{\sigma_1} \times \cdots \times E_{\sigma_n})$. On définit $\bar{\varepsilon}_\sigma$ (valeur de ε_σ dans $\mathfrak{M}^\tau$) en posant $\bar{\varepsilon}_\sigma = \{(a_1, ..., a_n, a)\,;\, a_1 \in E_{\sigma_1}, ..., a_n \in E_{\sigma_n}\,;\, a \in E_\sigma\,;\, (a_1, ..., a_n) \in \varphi_\sigma(a)\}$. Les « éléments » de $a \in E_\sigma$ dans $\mathfrak{M}^\tau$ sont donc les éléments de $\varphi_\sigma(a)$. Comme φ_σ est une bijection, on voit immédiatement que l'axiome d'extensionnalité d'ordre σ est satisfait. On a donc défini une réalisation $\mathfrak{M}^\tau$ d'ordre τ de $\mathscr{L}$, construite sur $\mathfrak{M}$, si on donne pour valeur aux symboles fonctionnels de $\mathscr{L}$ et aux symboles relationnels différents de ε_σ celle qu'ils avaient dans $\mathfrak{M}$.

Soit $\mathfrak{N}^\tau$ une réalisation d'ordre τ de $\mathscr{L}$, construite sur $\mathfrak{M}$, et F_σ ($\sigma \leqslant \tau$) ses ensembles de base. On a donc $F_0 = E_0$. On définit par récurrence sur le rang de σ une injection i_σ de F_σ dans E_σ : i_0 est l'identité ; si $\sigma = (\sigma_1, ..., \sigma_n)$, pour tout $a \in F_\sigma$ soit

$$\hat{a} = \{(a_1, ..., a_n) \in F_{\sigma_1} \times \cdots \times F_{\sigma_n}\,;\, (a_1, ..., a_n) \text{ est un « élément » de } a \text{ dans } \mathfrak{N}^\tau\}.$$

D'après l'axiome d'extensionnalité d'ordre σ, l'application $a \to \hat{a}$ est une injection de F_σ dans

$$\mathfrak{P}(F_{\sigma_1} \times \cdots \times F_{\sigma_n}).$$

Des injections

$$i_{\sigma_1} : F_{\sigma_1} \to E_{\sigma_1}\,; \ldots ;\, i_{\sigma_n} : F_{\sigma_n} \to E_{\sigma_n}\,,$$

déjà définies d'après l'hypothèse de récurrence on déduit une injection j :

$$\mathfrak{P}(F_{\sigma_1} \times \cdots \times F_{\sigma_n}) \to \mathfrak{P}(E_{\sigma_1} \times \cdots \times E_{\sigma_n}) .$$

On pose $i_\sigma(a) = \varphi_\sigma^{-1} \circ j(\hat{a})$; i_σ est bien une injection car c'est une composée d'injections. D'après sa définition il est clair que $(a_1, ..., a_n)$ est un « élément » de a dans $\mathfrak{N}^\tau$ si et seulement si $(i_{\sigma_1}(a_1), ..., i_{\sigma_n}(a_n))$ est un « élément » de $i_\sigma(a)$ dans $\mathfrak{M}^\tau$. L'ensemble des applications $i_\sigma (\sigma \leqslant \tau)$ constitue donc un plongement de $\mathfrak{N}^\tau$ dans $\mathfrak{M}^\tau$ qui conserve $\mathfrak{M}$.

La réalisation $\mathfrak{M}^\tau$ satisfait donc les conditions du théorème. Soit $\mathfrak{N}^\tau$ une autre réalisation d'ensembles de base F_σ $(\sigma \leqslant \tau)$, satisfaisant ces conditions. Alors, en particulier $\mathfrak{M}^\tau$ se plonge dans $\mathfrak{N}^\tau$ par une injection i qui conserve chaque élément de $E_0 = F_0$ (ensemble de base de $\mathfrak{M}$) et qui est compatible avec les valeurs des ε_σ dans $\mathfrak{M}^\tau$ et $\mathfrak{N}^\tau$.

Soit $\sigma = (\sigma_1, ..., \sigma_n)$ un type de rang minimum pour lequel i n'est pas un isomorphisme ; comme i est une injection, il y a un élément b de F_σ qui n'est l'image d'aucun élément de E_σ. Les « éléments » de b dans $\mathfrak{N}^\tau$ sont de la forme $(b_1, ..., b_n)$, avec $b_1 \in F_{\sigma_1}, ..., b_n \in F_{\sigma_n}$. Comme $\sigma_k < \sigma$ $(1 \leqslant k \leqslant n)$ il existe $a_1 \in E_{\sigma_1}, ..., a_n \in F_{\sigma_n}$ tels que $i(a_k) = b_k$ pour $1 \leqslant k \leqslant n$. D'après la construction de $\mathfrak{M}^\tau$, on peut définir $a \in E_\sigma$ en posant

$$a = \varphi_\sigma^{-1} \{(i^{-1} b_1, ..., i^{-1} b_n) ; (b_1, ..., b_n) \text{ est un « élément » de } b \text{ dans } \mathfrak{N}^\tau\}.$$

Alors $i(a)$ et b ont les mêmes « éléments » dans $\mathfrak{N}^\tau$, ce qui contredit l'axiome d'extensionnalité.

C. q. f. d.

Remarque. — En général, une réalisation non principale $\mathfrak{N}^\tau$ construite sur $\mathfrak{M}$ peut se plonger de plusieurs façons dans la réalisation principale $\mathfrak{M}^\tau$. Par exemple si $E_0 = \{0, 1\}$, $F_{(0)} = \{\{0\}\}$, $F_{((0))} = \{\{\{0\}\}\}$, l'application suivante constitue un plongement de $\mathfrak{N}^{((0))}$ dans $\mathfrak{M}^{((0))}$ distinct de l'application identique :

$$0 \to 0 , \quad 1 \to 1 , \quad \{0\} \to \{0\} , \quad \{\{0\}\} \to \{\{0\}, \{1\}\} .$$

En effet $\{\{0\}, \{1\}\}$ n'a pas d'autre « élément » dans $\mathfrak{N}^{((0))}$ que $\{0\}$.

Le plongement particulier i_σ $(\sigma \leqslant \tau)$ construit dans la démonstration du théorème sera appelé *plongement canonique* de $\mathfrak{N}^\tau$ dans $\mathfrak{M}^\tau$.

Supposons maintenant le langage $\mathscr{L}$ réduit au seul symbole $=$. Une réalisation de $\mathscr{L}$ est alors simplement la donnée d'un ensemble $E \neq \phi$. Nous désignerons par $\mathfrak{M}^\tau(E)$ la réalisation principale d'ordre τ construite sur E ; on l'appelle aussi *échelle des types simples* $\leqslant \tau$ sur l'ensemble E (l'adjectif « simples » exprime que les ensembles de base des divers types sont disjoints deux à deux). Toute réalisation $\mathfrak{N}^\tau(E)$ d'ordre τ construite sur E se plonge canoniquement dans $\mathfrak{M}^\tau(E)$ d'après le théorème précédent.

Soient E, F deux ensembles non vides, tels que $E \subset F$. Il est clair que toute réalisation d'ordre τ construite sur E, et en particulier la réalisation principale

$\mathfrak{M}^\tau(E)$ devient une réalisation d'ordre τ construite sur E si on ajoute $F - E$ à l'ensemble de base de type 0 de $\mathfrak{M}^\tau(E)$. D'où un plongement canonique de $\mathfrak{M}^\tau(E)$ dans $\mathfrak{M}^\tau(F)$ qui prolonge l'injection de E dans F. Soient alors $\mathfrak{R}^\tau(E)$ et $\mathfrak{R}^\tau(F)$ deux réalisations d'ordre τ construites respectivement sur E et sur F. On a les 3 injections canoniques α, β, γ :

$$\mathfrak{R}^\tau(E) \xrightarrow{\alpha} \mathfrak{M}^\tau(E) \xrightarrow{\beta} \mathfrak{M}^\tau(F)$$

$$\mathfrak{R}^\tau(F) \xrightarrow{\gamma} \mathfrak{M}^\tau(F) .$$

On dira que $\mathfrak{R}^\tau(F)$ *est une τ-extension de* $\mathfrak{R}^\tau(E)$ si et seulement si $\gamma\mathfrak{R}^\tau(F)$ est une extension (au sens des réalisations du langage $\mathscr{L}^\tau$) de $\beta\alpha\mathfrak{R}^\tau(E)$.

Soient maintenant E et F deux ensembles tels que $E \cap F \neq \phi$, et soient $\mathfrak{R}^\tau(E)$, $\mathfrak{R}^\tau(F)$ deux réalisations d'ordre τ construites respectivement sur E et sur F. $\mathfrak{M}^\tau(E \cap F)$ étant la réalisation principale d'ordre τ construite sur $E \cap F$, on a les injections canoniques α_1, β_1, α_2, β_2 :

$$\mathfrak{R}^\tau(E) \xrightarrow{\alpha_1} \mathfrak{M}^\tau(E) \xleftarrow{\beta_1} \mathfrak{M}^\tau(E \cap F)$$

$$\mathfrak{R}^\tau(F) \xrightarrow{\alpha_2} \mathfrak{M}^\tau(F) \xleftarrow{\beta_2} \mathfrak{M}^\tau(E \cap F) .$$

On appelle *τ-intersection de* $\mathfrak{R}^\tau(E)$ *et* $\mathfrak{R}^\tau(F)$ la réalisation $\mathfrak{R}^\tau(E \cap F)$ d'ordre τ construite sur $E \cap F$, définie de la façon suivante : $\mathfrak{R}^\tau(E \cap F)$ est une sous-réalisation de $\mathfrak{M}^\tau(E \cap F)$; si $\xi \in \mathfrak{M}^\tau(E \cap F)$, alors $\xi \in \mathfrak{R}^\tau(E \cap F)$ si et seulement si $\beta_1\xi \in \alpha_1\mathfrak{R}^\tau(E)$ et $\beta_2\xi \in \alpha_2\mathfrak{R}^\tau(F)$.

Ces deux définitions s'étendent aisément au cas général où $\mathscr{L}$ est un langage égalitaire à un seul type d'objets. En effet si $\mathfrak{M}$ est une réalisation de $\mathscr{L}$ d'ensemble de base E, la donnée d'une réalisation d'ordre τ construite sur $\mathfrak{M}$ équivaut à la donnée de $\mathfrak{M}$ et d'une réalisation $\mathfrak{R}^\tau(E)$ d'ordre τ construite sur E. Donc, étant données $\mathfrak{M}$ et $\mathfrak{N}$, réalisations de $\mathscr{L}$ d'ensembles de base respectifs E et F, soient $(\mathfrak{M}, \mathfrak{R}^\tau(E))$ et $(\mathfrak{N}, \mathfrak{R}^\tau(F))$ deux réalisations d'ordre τ de $\mathscr{L}$ construites respectivement sur $\mathfrak{M}$ et $\mathfrak{N}$. On dira que $(\mathfrak{N}, \mathfrak{R}^\tau(F))$ *est une τ-extension de* $(\mathfrak{M}, \mathfrak{R}^\tau(E))$ si et seulement si $\mathfrak{N}$ est une extension de $\mathfrak{M}$ et $\mathfrak{R}^\tau(F)$ une τ-extension de $\mathfrak{R}^\tau(E)$.

Si $\mathfrak{M}$ et $\mathfrak{N}$ coïncident sur $E \cap F$, supposé non vide, (c'est-à-dire si les valeurs des symboles relationnels et fonctionnels de $\mathscr{L}$ dans $\mathfrak{M}$ et $\mathfrak{N}$ coïncident sur $E \cap F$), $\mathfrak{M} \cap \mathfrak{N}$ est une réalisation de $\mathscr{L}$ d'ensemble de base $E \cap F$. On appelle *τ-intersection de* $(\mathfrak{M}, \mathfrak{R}^\tau(E))$ *et de* $(\mathfrak{N}, \mathfrak{R}^\tau(F))$ la réalisation d'ordre τ de $\mathscr{L}$ construite sur $\mathfrak{M} \cap \mathfrak{N}$ donnée par le couple $(\mathfrak{M} \cap \mathfrak{N}, \mathfrak{R}^\tau(E \cap F))$ où $\mathfrak{R}^\tau(E \cap F)$ est la τ-intersection de $\mathfrak{R}^\tau(E)$ et $\mathfrak{R}^\tau(F)$.

EXERCICES

1. (Langages à k types d'objets avec symboles fonctionnels.)

1° Donner une définition des ensembles de termes $T^{(1)}, \ldots, T^{(k)}$ de $\mathscr{L}$, langage à k types d'objets avec symboles fonctionnels. Montrer

qu'étant donnée une réalisation égalitaire de $\mathcal{L}$, d'ensembles de base $U_1, \dots, U_k$, chaque élément δ de $U_1^{V_{\mathcal{L}}^{(1)}} \times \cdots \times U_k^{V_{\mathcal{L}}^{(k)}}$ se prolonge d'une façon et d'une seule en une application $\hat{\delta}$ de $T^{(i)}$ dans U_i (pour chaque i, $1 \leqslant i \leqslant k$), ayant les propriétés suivantes :

a) $\hat{\delta}(x^{(i)}) = \delta(x^{(i)})$ pour chaque variable $x^{(i)}$.

b) $\hat{\delta}(ft_1 \dots t_n) = f(\hat{\delta}(t_1), \dots, \hat{\delta}(t_n))$ pour chaque symbole fonctionnel f de type $(i, i_1 \dots i_n)$ et chaque suite de termes $t_1, \dots, t_n$ de types respectifs $i_1, \dots, i_n$.

2° On désigne par $\mathcal{L}_0$ le langage égalitaire à k types d'objets sans symboles fonctionnels, ayant tous les symboles relationnels de $\mathcal{L}$ (avec le même nombre de variables et les mêmes types) et qui, pour chaque symbole fonctionnel f de type $(i, i_1, \dots, i_n)$ de $\mathcal{L}$, possède un symbole relationnel S_f de type $(i, i_1, \dots, i_n)$. Les symboles S_f sont supposés distincts entre eux, et distincts des précédents. A chaque formule F de $\mathcal{L}_0$ correspond une formule F^* de $\mathcal{L}$, obtenue en substituant à chaque formule atomique de la forme $S_f\, x^{(i)}\, x_1^{(i_1)} \dots x_n^{(i_n)}$ qui apparaît dans F, la formule $x^{(i)} = fx_1^{(i_1)} \dots x_n^{(i_n)}$.

Montrer que pour toute formule Φ de $\mathcal{L}$, il existe une formule équivalente de $\mathcal{L}$, qui a les mêmes symboles relationnels (l'égalité mise à part) et fonctionnels, et les mêmes types que Φ, et qui est de la forme F^*.

3° On désigne par $\mathcal{A}_0$ l'ensemble des formules suivantes de $\mathcal{L}_0$:

$$\bigwedge x_1^{(i_1)} \dots \bigwedge x_n^{(i_n)} \bigvee x^{(i)}\, S_f\, x^{(i)}\, x_1^{(i_1)} \dots x_n^{(i_n)} .$$

$$\bigwedge x_1^{(i_1)} \dots \bigwedge x_n^{(i_n)} \bigwedge x^{(i)} \bigwedge y^{(i)} [S_f\, x^{(i)}\, x_1^{(i_1)} \dots x_n^{(i_n)} \wedge$$
$$\wedge\; S_f\, y^{(i)}\, x_1^{(i_1)} \dots x_n^{(i_n)} \rightarrow x^{(i)} = y^{(i)}] .$$

pour chaque symbole fonctionnel f (de type $(i, i_1, \dots, i_n)$) de $\mathcal{L}$. Etablir une correspondance biunivoque entre les modèles égalitaires de $\mathcal{A}_0$ et les réalisations de $\mathcal{L}$, telle que si $\mathfrak{M}$ est une réalisation de $\mathcal{L}$, $\mathfrak{M}_0$ le modèle correspondant de $\mathcal{A}_0$, et F une formule close de $\mathcal{L}_0$, alors F est satisfaite par $\mathfrak{M}_0$ si et seulement si F^* l'est par $\mathfrak{M}$.

En déduire le théorème de finitude et le théorème d'interpolation pour le langage $\mathcal{L}$.

Solution :

1° Soit Z l'ensemble des schémas fonctionnels construits à l'aide des éléments de $V_{\mathcal{L}}^{(1)} \cup \cdots \cup V_{\mathcal{L}}^{(k)}$ comme symboles à 0 variables, et des éléments de $\mathrm{F}_{\mathcal{L}}^{(i, i_1, \dots, i_n)}$ comme symboles à n variables (pour chaque suite $i, i_1, \dots, i_n$ d'entiers compris entre 1 et k).

Un élément ξ de Z sera dit de type i si $\xi \in V_{\mathcal{L}}^{(i)}$ ou si ξ commence par un symbole fonctionnel $f \in \mathrm{F}_{\mathcal{L}}^{(i, i_1, \dots, i_n)}$ (symbole fonctionnel à valeurs de

type i). Désignons par $Z^{(i)}$ l'ensemble des schémas de type i. Alors les $Z^{(i)}$ sont disjoints deux à deux et on a $Z = Z^{(1)} \cup \cdots \cup Z^{(k)}$.

On définit une application J de Z dans $\{0, 1\}$ par récurrence sur la longueur de la façon suivante :

— $J(x) = 1$ pour chaque variable x de $\mathscr{L}$;

— si $\xi \in Z$, ξ s'écrit d'une façon et d'une seule sous la forme $f\xi_1 \dots \xi_n$ avec $f \in \mathrm{F}_{\mathscr{L}}^{(i,i_1,\dots,i_n)}$ et $\xi_1, \dots, \xi_n \in Z$ (sauf si ξ est une variable, cas que l'on vient d'examiner). On pose alors :

$J(\xi) = 1$ si $J(\xi_1) = \cdots = J(\xi_n) = 1$, et si $\xi_1, \dots, \xi_n$ sont de types respectifs $i_1, \dots, i_n$.

$J(\xi) = 0$ sinon.

L'ensemble T des termes de $\mathscr{L}$ est par définition l'ensemble des $\xi \in Z$ tels que $J(\xi) = 1$. L'ensemble $T^{(i)}$ des termes de type i de $\mathscr{L}$ est $T \cap Z^{(i)}$, c'est-à-dire l'ensemble des termes qui commencent par un symbole fonctionnel à valeur de type i.

— *Pour que t soit un terme de type i, il faut et il suffit qu'il soit une variable de type i, ou que $t = ft_1 \dots t_n$ avec $f \in \mathrm{F}_{\mathscr{L}}^{(i,i_1,\dots,i_n)}$, $t_1, \dots, t_n$ étant des termes de types respectifs $i_1, \dots, i_n$; f, $t_1, \dots, t_n$ sont alors déterminés de façon unique.*

Car si $t \in T^{(i)}$, on a $t \in Z$, donc t est une variable, ou bien

$$t = ft_1 \dots t_n \,, \quad \text{avec} \quad f \in T_{\mathscr{L}}^{(i,i_1,\dots,i_n)} \quad \text{et} \quad t_1, \dots, t_n \in Z \,.$$

De plus f, $t_1, \dots, t_n$ sont déterminés de façon unique (Préliminaires). Comme $J(t) = 1$, on a

$$J(t_1) = \cdots = J(t_n) = 1 \,,$$

ce qui montre que $t_1, \dots, t_n$ sont des termes de types respectifs $i_1, \dots, i_n$. Inversement si $t_1, \dots, t_n$ sont des termes de types respectifs $i_1, \dots, i_n$ et si $f \in \mathrm{F}_{\mathscr{L}}^{(i,i_1,\dots,i_n)}$ alors $ft_1 \dots t_n$ est un terme de type i puisque $J(ft_1 \dots t_n) = 1$.

— Soit alors $\mathfrak{M}$ une réalisation de $\mathscr{L}$, d'ensembles de base $U_1, \dots, U_k$. Pour chaque $f \in \mathrm{F}_{\mathscr{L}}^{(i,i_1,\dots,i_n)}$, soit $\bar{f}$ sa valeur dans $\mathfrak{M}$; $\bar{f}$ est une application de $U_{i_1} \times \cdots \times U_{i_n}$ dans U_i. Donnons-nous une application δ, qui pour chaque i ($1 \leqslant i \leqslant k$) envoie $V_{\mathscr{L}}^{(i)}$ dans U_i. On définit le prolongement $\hat{\delta}$ de δ à l'ensemble des termes, par récurrence sur la longueur : si $t = ft_1 \dots t_n$ est un terme de type i (avec $f \in \mathrm{F}_{\mathscr{L}}^{(i,i_1,\dots,i_n)}$, $t_1 \in T^{(i_1)}, \dots, t_n \in T^{(i_n)}$), alors

$$\hat{\delta}(t) = \bar{f}\,(\hat{\delta}(t_1), \dots, \hat{\delta}(t_n)) \,.$$

On vérifie immédiatement que ce prolongement est une application de $T^{(i)}$ dans U_i pour chaque i ($1 \leqslant i \leqslant k$) qui satisfait la condition imposée.

2° Supposons que Φ soit une formule atomique de $\mathscr{L}$ de la forme $x^{(i)} = t^{(i)}$, où $x^{(i)}$ est une variable de type i et $t^{(i)}$ un terme de type i. On montre par récurrence sur la longueur de $t^{(i)}$ que Φ équivaut à une formule de la forme F^*. C'est évident si $t^{(i)}$ est de longueur 1 : car alors $t^{(i)}$ est soit une variable, soit un symbole de constante de type i.

Si $t^{(i)}$ est de longueur $v > 1$, on a

$$t^{(i)} = ft_1^{(i_1)} \dots t_n^{(i_n)}, \qquad \text{avec} \qquad f \in \mathrm{F}^{(i,i_1,\dots,i_n)^*},$$

$t_1^{(i_1)}, \dots, t_n^{(i_n)}$ étant des termes de types respectifs $i_1, \dots, i_n$. Alors $x^{(i)} = t^{(i)}$ équivaut à

$$\bigvee x_1^{(i_1)} \dots \bigvee x_n^{(i_n)} [x_1^{(i_1)} = t_1^{(i_1)} \wedge \cdots \wedge x_n^{(i_n)} = t_n^{(i_n)} \wedge x^{(i)} = fx_1^{(i_1)} \dots x_n^{(i_n)}] .$$

Par hypothèse

$$x_1^{(i_1)} = t_1^{(i_1)}, \dots, x_n^{(i_n)} = t_n^{(i_n)}$$

sont respectivement équivalentes à $F_1^*, \dots, F_n^*$; donc $x^{(i)} = t^{(i)}$ équivaut à

$$\bigvee x_1^{(i_1)} \dots \bigvee x_n^{(i_n)} [F_1^* \wedge \cdots \wedge F_n^* \wedge x^{(i)} = fx_1^{(i_1)} \dots x_n^{(i_n)}] ,$$

c'est-à-dire à F^*, où F est la formule de $\mathscr{L}_0$:

$$\bigvee x_1^{(i_1)} \dots \bigvee x_n^{(i_n)} [F_1 \wedge \cdots \wedge F_n \wedge S_f \, x^{(i)} x_1^{(i_1)} \dots x_n^{(i_n)}] .$$

De plus les symboles fonctionnels et les types qui apparaissent dans la formule $x^{(i)} = t^{(i)}$ sont ceux qui apparaissent dans les formules

$$x_1^{(i_1)} = t_1^{(i_1)}, \dots, x_n^{(i_n)} = t_n^{(i_n)}, x^{(i)} = fx_1^{(i_1)} \dots x_n^{(i_n)} ;$$

D'après l'hypothèse de récurrence, ce sont ceux qui apparaissent dans

$$F_1^*, \dots, F_n^*, x^{(i)} = fx_1^{(i_1)} \dots x_n^{(i_n)} ,$$

donc ceux qui figurent dans F^*.

— Soit maintenant Φ une formule atomique quelconque de $\mathscr{L}$. Φ s'écrit $Rt_1^{(i_1)} \dots t_n^{(i_n)}$, où R est un symbole relationnel à n variables

$$(R \in \mathrm{R}_{\mathscr{L}}^{(n)} \quad \text{ou} \quad R \in \mathrm{S}_{\mathscr{L}}^{(i_1,\dots,i_n)}) \qquad \text{et} \qquad t_1^{(i_1)}, \dots, t_n^{(i_n)}$$

sont des termes de types respectifs à $i_1, \dots, i_n$.

Alors Φ équivaut à

$$\bigvee x_1^{(i_1)} \dots \bigvee x_n^{(i_n)} [x_1^{(i_1)} = t_1^{(i_1)} \wedge \cdots \wedge x_n^{(i_n)} = t_n^{(i_n)} \wedge Rx_1^{(i_1)} \dots x_n^{(i_n)}] .$$

Comme $x_1^{(i_1)} = t_1^{(i_1)}$ équivaut à $F_1^*, \dots, x_n^{(i_n)} = t_n^{(i_n)}$ équivaut à F_n^*, Φ équivaut à F^* où F est la formule

$$\bigvee x_1^{(i_1)} \dots \bigvee x_n^{(i_n)} [F_1 \wedge \cdots \wedge F_n \wedge Rx_1^{(i_1)} \dots x_n^{(i_n)}] .$$

De plus les symboles relationnels et fonctionnels, et les types de F^* sont ceux de Φ (l'égalité mise à part). On montre alors, par récurrence sur la longueur de Φ, que toute formule Φ de $\mathscr{L}$ équivaut à une formule F^* qui a les mêmes symboles relationnels et fonctionnels et les mêmes types que Φ : si $\Phi = \Phi_1 \vee \Phi_2$, Φ_1 et Φ_2 sont respectivement équivalentes à F_1^* et F_2^*, donc Φ équivaut à $F_1^* \vee F_2^*$, c'est-à-dire à $(F_1 \vee F_2)^*$; même démonstration si $\Phi = \neg \Phi_1$, ou si $\Phi = \forall x \Phi_1$.

3° Si $\mathfrak{M}_0$ est un modèle égalitaire de $\mathscr{A}_0$, d'ensembles de base $U_1, ..., U_k$, et f un symbole fonctionnel de $\mathscr{L}$ de type $(i, i_1, ..., i_n)$, la valeur de S_f dans $\mathfrak{M}_0$ est le graphe d'une application de $U_{i_1} \times \cdots \times U_{i_n}$ dans U_i. D'où une réalisation $\mathfrak{M}$ de $\mathscr{L}$, qui a les mêmes ensembles de base. Il est clair que toute réalisation de $\mathscr{L}$ est ainsi obtenue, et qu'une formule F de $\mathscr{L}_0$ est satisfaite dans $\mathfrak{M}_0$ si et seulement si F^* est satisfaite par $\mathfrak{M}$.
— Soit alors $\mathscr{B}$ un ensemble de formules closes de $\mathscr{L}$ tel que tout sous-ensemble fini ait un modèle. On peut supposer que chaque formule de $\mathscr{B}$ est de la forme F^* où F est une formule de $\mathscr{L}_0$ (d'après la 2e question). Soit $\mathscr{B}_0$ l'ensemble des formules F de $\mathscr{L}_0$ telles que $F^* \in \mathscr{B}$. Si $\{ F_1, ..., F_n \}$ est un sous-ensemble fini de $\mathscr{B}_0$, $\{ F_1^*, ..., F_n^* \}$ a un modèle par hypothèse, ce qui montre que $(\mathscr{A}_0, F_1, ..., F_n)$ a un modèle. Le théorème de finitude pour le langage $\mathscr{L}_0$ montre alors que $(\mathscr{A}_0, \mathscr{B}_0)$ a un modèle $\mathfrak{M}_0$. La réalisation $\mathfrak{M}$ de $\mathscr{L}$ qui correspond à $\mathfrak{M}_0$ satisfait $\mathscr{B}$. Cela montre le théorème de finitude pour le langage $\mathscr{L}$.
Soient maintenant F, G deux formules de $\mathscr{L}$ telles que $F \wedge G$ n'ait pas de modèle. Il existe deux formules A et B de $\mathscr{L}_0$, telles que A^* (resp. B^*) soit équivalente à F (resp. G) et ait les mêmes symboles relationnels (l'égalité mise à part) les mêmes symboles fonctionnels et les mêmes types que F (resp. G). Soient $\mathscr{A}_1$ le sous-ensemble de $\mathscr{A}_0$ qui correspond aux symboles fonctionnels qui figurent dans A^*, $\mathscr{A}_2$ celui qui correspond aux symboles fonctionnels de B^*. Les types qui figurent dans $\mathscr{A}_1$ (resp. A_2) figurent aussi dans A^* (resp. B^*).
Comme $A^* \wedge B^*$ n'a pas de modèle, $(A, B, \mathscr{A}_1, \mathscr{A}_2)$ n'en a pas non plus. Le théorème d'interpolation pour le langage égalitaire $\mathscr{L}_0$, appliqué aux formules $\mathscr{A}_1 \wedge A$, $\mathscr{A}_2 \wedge B$, donne une formule H dont les symboles relationnels et les types sont communs à A et B et telle que $\mathscr{A}_1, A \vdash H$; $\mathscr{A}_2, B \vdash \neg H$. On en déduit que $A^* \vdash H^*$ et $B^* \vdash \neg H^*$; donc $F \vdash H^*$ et $G \vdash \neg H^*$. Cela montre le théorème d'interpolation pour le langage $\mathscr{L}$.

2. (*Relation entre les méthodes des chapitres* 2 *et* 5).

Soit $\mathscr{L}$ un langage à un seul type d'objets, sans symboles fonctionnels. On définit $\mathscr{L}_\Delta$ et Ω de la façon indiquée dans ce chapitre. Soit F une formule de $\mathscr{L}$, $\hat{F}$ la formule universelle construite à partir de F, au chapitre 2. Le langage de $\hat{F}$ est donc celui de F augmenté d'un nombre fini de symboles fonctionnels $\varphi_1, ..., \varphi_m$.

Définir des fonctions $f_1, ..., f_m$ sur Δ, ayant respectivement le même nombre d'arguments que $\varphi_1, ..., \varphi_m$, et telles que, si $\mathfrak{M}$ est un modèle canonique de Ω, et si on le complète en une réalisation de $\mathscr{L}(\hat{F})$ en donnant les valeurs respectives $f_1, ..., f_m$ aux symboles fonctionnels $\varphi_1, ..., \varphi_m$, on ait $\overline{\hat{F}} = \overline{F}$ dans la réalisation ainsi obtenue.

Solution.

On suppose que F est une formule prénexe de $\mathscr{L}$ (non forcément close) et on définit l'ensemble $\{f_1, ..., f_m\}$ par récurrence sur le nombre de quantificateurs de F. Si F est sans quantificateur, $\hat{F} = F$, et il n'y a rien à définir.

— Si $F = \bigwedge x G(x, x_1, ..., x_n)$, on a $\hat{F} = \bigwedge x \hat{G}$. Les symboles fonctionnels $\varphi_1, ..., \varphi_m$ de $\hat{F}$ sont donc ceux de $\hat{G}$, et on leur donne les valeurs $f_1, ..., f_m$ qui ont déjà été définies pour G. On a bien $\overline{\hat{F}} = \overline{F}$, puisque $\overline{\hat{G}} = \overline{G}$.

— Si $F = \bigvee x G(x, x_1, ..., x_n)$, soient $\varphi_1, ..., \varphi_m$ les symboles fonctionnels de $\hat{G}$. Alors

$$\hat{F} = \hat{G}(\varphi x_1 ..., x_n, x_1, ... x_n)\,,$$

où φ est un nouveau symbole fonctionnel à n variables. On donne à $\varphi_1, ..., \varphi_m$ les valeurs $f_1, ..., f_m$ qui ont déjà été définies pour G. Et on définit f par

$$f(a_1, ..., a_n) = \varepsilon G(x, a_1, ..., a_n)$$

pour $a_1, ..., a_n \in \Delta$.
Alors

$$(a_1, ..., a_n) \in \overline{\hat{F}} \Leftrightarrow (f(a_1, ..., a_n), a_1, ..., a_n) \in \overline{\hat{G}}$$
$$\Leftrightarrow (f(a_1, ..., a_n), a_1, ..., a_n) \in \overline{G}\,, \qquad \text{puisque} \qquad \overline{\hat{G}} = \overline{G}\,.$$

Donc

$$(a_1, ..., a_n) \in \overline{\hat{F}} \Leftrightarrow \quad \mathfrak{M} \text{ satisfait } \quad G(a, a_1, ..., a_n)\,,$$

avec $a = \varepsilon G(x, a_1, ..., a_n)$.
Comme $\mathfrak{M}$ satisfait Ω on a donc

$$(a_1, ..., a_n) \in \overline{\hat{F}} \Leftrightarrow \quad \mathfrak{M} \text{ satisfait } \quad \bigvee x G(x, a_1, ..., a_n)$$

et donc $\overline{\hat{F}} = \overline{F}$.

3. *Compléments au théorème d'uniformité* (pour le calcul des prédicats à plusieurs types de variables avec symboles fonctionnels).

a) Montrer que, si $\bigvee x_1 ... \bigvee x_n\, A$, A sans quantificateur est valide, alors

il existe une suite de n-uplets $(t_1^{(i)}, ..., t_n^{(i)})$ $(1 \leqslant i \leqslant p)$ de termes du langage de A, $t_j^{(i)}$ étant du même type que x_j $(1 \leqslant i \leqslant p, 1 \leqslant j \leqslant n)$, telle que $A_1 \vee \cdots \vee A_p$ soit valide, A_i étant obtenue en remplaçant x_j dans A par $t_j^{(i)}$.

b) En déduire que, si $\mathcal{U}'$ est un ensemble de formules prénexes dont tous les quantificateurs sont universels et si la formule existentielle E est conséquence de $\mathcal{U}'$, alors il existe une formule A sans quantificateur telle que $\mathcal{U}' \vdash A$ et $A \rightarrow E$.

c) Déduire de *b*) que si $\mathcal{U}$ est un ensemble de formules universelles, si U est une formule universelle et si $\mathcal{U} \vdash (U \leftrightarrow E)$ alors il existe une formule B sans quantificateurs telle que $\mathcal{U} \vdash (U \leftrightarrow B)$ et $\mathcal{U} \vdash (B \leftrightarrow E)$.

Solution.

a) On considère les réalisations canoniques du langage $\mathcal{L}$ de A ; alors l'ensemble de base de type p est l'ensemble de tous les termes de type p de $\mathcal{L}$ sans variable. (Si $\mathcal{L}$ ne contient pas de symbole de constante on considère tous les termes de type p de $\mathcal{L} \cup \{ a \}$ où a est un nouveau symbole de constante). Puisque $\bigvee x_1 ... \bigvee x_n A$ est un théorème, l'ensemble des formules $\{ \neg A_1, \neg A_2, ... \}$ n'a pas de modèle canonique. D'après le théorème de finitude pour le calcul propositionnel il existe donc un q tel que

$$\neg A_1 \wedge \neg A_2 \wedge \cdots \wedge \neg A_q$$

n'a pas de modèle, et par conséquent $A_1 \vee A_2 \vee \cdots \vee A_q$ est un théorème.

b) D'après le théorème de finitude il existe un sous-ensemble fini $\mathcal{U}_1$ de $\mathcal{U}'$ tel que $\mathcal{U}_1 \vdash E$. La conjonction des formules de $\mathcal{U}_1$ équivaut à une formule universelle, soit $\bigwedge y_1 ... \bigwedge y_r C$. Si $E = \bigvee z_1 ... \bigvee z_s D$ (C et D sans quantificateurs),

$$\bigvee y_1 ... \bigvee y_r \bigvee z_1 ... \bigvee z_s(\neg C \vee D)$$

est un théorème. D'après *a*), une formule de la forme

$$\neg C_1 \vee \neg C_2 \vee \cdots \vee \neg C_q \vee D_1 \vee \cdots \vee D_q$$

est un théorème. On prend $D_1 \vee \cdots \vee D_q$ pour A. Puisque

$$\vdash \bigwedge y_1 ... \bigwedge y_r C \rightarrow (C_1 \wedge \cdots \wedge C_q),$$

et

$$\mathcal{U}' \vdash \bigwedge y_1 ... \bigwedge y_r C,$$

on voit que

$$\mathcal{U}' \vdash (D_1 \vee \cdots \vee D_q) ;$$

puisque $D_i \to E$ pour tout i $(1 \leqslant i \leqslant q)$, $(D_1 \vee \cdots \vee D_q) \to E$ est valide.

c) On prend $\mathscr{U}' = \mathscr{U} \cup \{ U \}$ dans *b*). Puisque $\mathscr{U}' \vdash E$, le *b*) donne une formule A qu'on prend pour B. Alors $\mathscr{U}' \vdash B$ et donc $\mathscr{U} \vdash (U \to B)$; $B \to E$ est un théorème et donc $\mathscr{U} \vdash (U \leftrightarrow B)$, $\mathscr{U} \vdash (E \leftrightarrow B)$.

4. *Compléments au lemme d'interpolation* (pour un langage $\mathscr{L}$ à plusieurs types de variables avec symboles fonctionnels).
Soient $U = \wedge x_1 \ldots \wedge x_m\, A$ et $E = \vee y_1 \ldots \vee y_n\, B$, où A et B sont deux formules de $\mathscr{L}$ sans quantificateurs, telles qu'aucune variable y ne figure dans A et aucune variable x ne figure dans B.

a) Déduire du lemme d'interpolation pour le calcul propositionnel construit sur les formules atomiques de $\mathscr{L}$ que, si $E \to U$ est un théorème, il existe une formule sans quantificateur C telle que $E \to C$ et $C \to U$ soient des théorèmes.

b) Soient F et G deux formules closes de $\mathscr{L}$ telles que $F \to G$ soit valide. Déduire du lemme d'interpolation qu'il existe une formule H telle que $\mathscr{L}(H) \subset \mathscr{L}(F) \cap \mathscr{L}(G)$ et $F \to H$ et $H \to G$ soient des théorèmes.

c) Trouver deux formules F et G d'un langage égalitaire telles que $\vdash (F \to G)$, G ne contient pas le symbole $=$, et telles qu'il n'existe aucune formule H ne contenant pas $=$, avec

$$\mathscr{L}(H) \subset \mathscr{L}(F) \cap \mathscr{L}(G), \vdash (F \to H) \text{ et } \vdash (H \to G).$$

Solution. — *a*) Puisque $\vdash E \to U$, la formule $B \to A$ est valide au sens du calcul propositionnel. Alors il existe une formule C construite sur les formules atomiques communes aux formules A et B telle que $B \to C$ et $C \to A$ soient des théorèmes. Par conséquent C ne contient que les variables communes à A et B, en particulier C ne contient ni les variables x, ni les variables y. Par conséquent $\vee y_1 \ldots \vee y_n\, B \to C$ et $C \to \wedge x_1 \ldots \wedge x_n\, A$ sont des théorèmes ce qui est le résultat cherché. (Par contre, si A et B sont deux formules du calcul des prédicats et $\vdash B \to A$, il n'existe pas forcément une C telle que $\vdash B \to C$, $\vdash C \to A$ qui ne contienne que les variables communes à B et A : p. ex. $B = Rx$ et $A = \vee y Ry$.)

b) D'après le lemme d'interpolation, il existe une formule H qui ne contient que les symboles relationnels et les symboles fonctionnels communs à $\mathscr{L}(F) \cap \mathscr{L}(G)$ telle que $\vdash F \to H$, $\vdash H \to G$. Supposons que H contienne une constante c qui ne figure pas dans F ; si u est une variable qui ne figure pas dans H et si H' est obtenue en remplaçant c par u dans H alors $\vdash F \to \wedge u H'$ et $\vdash \wedge u H' \to G$. Si la constante c ne figure pas dans G, alors $\vdash \vee u H' \to G$, et $\vdash F \to \vee u H'$. On élimine ainsi dans H toutes les constantes qui ne sont pas communes aux deux formules F et G.

c) Soit F la formule $\wedge x \wedge y (x = y)$. Alors $F \to (\wedge x Px \vee \wedge x \neg Px)$ est satisfaite (P est un symbole relationnel à un seul argument). Une

formule H satisfaisant les conditions de (*c*) serait ou bien $\top$ ou bien $\perp$ ce qui est absurde.

5. Pour tout entier n on définit le type *pur* d'ordre n par récurrence : 0 est le type des individus et $n + 1 = (n)$. Pour $n > 0$, si $\sigma \in [n]$, alors σ est aussi un type pur $m \leqslant n$, et le symbole relationnel ε_σ a deux arguments. Si $\mathscr{L}$ est un langage du premier ordre à un seul type de variable (et ne contenant pas le symbole ε), et si $n > 1$, $\mathscr{L}^n_\varepsilon$ est obtenu en ajoutant à $\mathscr{L}$ le symbole relationnel ε à deux variables et $n - 1$ types de variables $(1, 2, ..., n - 1)$.

Pour tout entier $n > 0$, on notera S_n (axiome de l'échelle des types $< n$ purs et simples) la conjonction des formules suivantes de $\mathscr{L}^n_\varepsilon$, où $i < n$, $j < n$, et où les variables x, y, z ont respectivement les types i, j, j, pour tout couple (i, j) :

$\bigwedge x \bigwedge y \neg x = y$, où $i < j$ (types simples),

$\bigwedge x \bigwedge y \neg x \varepsilon y$, où $j \neq i + 1$,

$\bigwedge y \bigwedge z[\bigwedge x(x\varepsilon y \leftrightarrow x \varepsilon z) \rightarrow y = z]$ où $j = i + 1$ (extensionnalité).

On notera S^ϕ_n la conjonction de S_n et des formules $\bigwedge y \bigvee x(x \varepsilon y)$ pour tout $i < n$ et $j = i + 1$ (tout ensemble vide est de type 0).

On notera C_n (axiome de l'échelle des types $< n$ cumulatifs) la conjonction des formules suivantes où les variables x, y, z ont respectivement les types i, j, k, pour tout couple (i, j) :

$\bigwedge x \bigvee y(y = x)$ où $j > i$ (types cumulatifs),

$\bigwedge x \bigwedge y \bigvee z(x \varepsilon y \rightarrow z = x)$, où $i \geqslant j$ et $j = k + 1$,

$\bigwedge y(\bigwedge x[x \varepsilon y \rightarrow \bigvee z(z = x)] \rightarrow \bigvee x(x = y))$, où $j = i + 1$ et $i = k + 1$,

$\bigwedge x \bigwedge y \neg x \varepsilon y$, où $j = 0$,

$\bigwedge x \bigwedge y[\bigwedge z(z \varepsilon x \leftrightarrow z \varepsilon y) \rightarrow x = y]$, où $k + 1 = \max(i, j)$.

a) Montrer comment passer (i) d'une $(n - 1)$ réalisation de $\mathscr{L}$ à un modèle de S_n (et inversement), (ii) d'un modèle de S^ϕ_n à un modèle de C_n (mais non inversement).

b) (Couples ordonnés de types simples). Pour tout couple d'entiers (i, j) trouver une formule $M_{i,j}$ à trois variables de type i, j, k respectivement avec $k = 2 + \max(i, j)$, telle que $\overline{M}_{i,j}$ soit une injection de $E_i \times E_j$ dans E_k pour toute réalisation de $\mathscr{L}^n_\varepsilon (n > k)$, dont les ensembles de base de type i, j, k sont respectivement E_i, E_j, E_k, satisfaisant S_n et la conjonction des formules suivantes :

$$\bigwedge x \bigwedge y \bigvee z \bigwedge u[u \varepsilon z \leftrightarrow (u = x \vee u = y)],$$

où x, y, u sont de type $r < k$, z de type $r + 1 (< n)$ (existence de cou-

ples). En déduire une injection de $E_{i_1} \times \cdots \times E_{i_p}$ dans E_k, où

$$k = N_p(i_1, ..., i_p),$$

N_p étant définie par :

$$N_2(i_1, i_2) = 2 + \max(i_1, i_2),$$

$$N_{p+1}(i_1, ..., i_{p+1}) = N_2(i_1, N_p(i_2, ..., i_{p+1})).$$

c) (Réduction des types finis aux types simples). Soit N la fonction définie sur l'ensemble **T** des types finis, en posant

$$N0 = 0, N\sigma = 1 + N\sigma_1, \text{ si } \sigma = (\sigma_1)$$

$$N\sigma = 1 + N_n(N\sigma_1, ..., N\sigma_n) \quad \text{si} \quad \sigma = (\sigma_1, ..., \sigma_n),$$

où N_n est la fonction définie au *b*). Pour tout type fini

$$\sigma = (\sigma_1, ..., \sigma_n)$$

trouver une formule M_σ de $\mathscr{L}^{(\sigma, N\sigma)}$ à 2 variables telle que $\overline{M}_\sigma$ soit une injection de l'ensemble de base E_σ dans $E_{N\sigma}$ pour toute réalisation principale de $\mathscr{L}^\tau(\sigma \in [\tau], N\sigma \in [\tau])$.

Solution.

a) (i) On prend pour $x \varepsilon y$ la disjonction des formules de $\mathscr{L}^n$

$$\bigvee x_i \bigvee x_{i+1}(x = x_i \wedge y = x_{i+1} \wedge x_i \,\varepsilon_{i+1}\, x_{i+1}), \quad \text{avec} \quad 0 < i + 1 < n,$$

où x_i est variable de type i. Si $E_0, ..., E_{n-1}$ sont les ensembles de base d'une réalisation de $\mathscr{L}^n$, $(E_0, ..., E_{n-1}, \bar{\varepsilon})$ est un modèle de S_n. Inversement, d'un modèle $(E_0, ..., E_{n-1}, \bar{\varepsilon})$ de S_n on déduit une n-réalisation de $\mathscr{L}^n$ en posant $x \varepsilon_{i+1} y = x \varepsilon y$ pourvu que x et y soient deux variables de type i, resp. $i + 1$.

(ii) Soit $(E_0, ..., E_{n-1}, \bar{\varepsilon})$ un modèle de S_n^ϕ. Si

$$E_0^c = E_0, E_{m+1}^c = E_m^c \cup E_{m+1} (m < n),$$

on a $E_i^c \supset E_j^c$ $(i > j)$; pour tout $\bar{x} \in E_m^c (m < n)$ il existe un seul i, noté $\mu(\bar{x})$, tel que $\bar{x} \in E_i$ (types simples) ; $\bar{x}\bar{\varepsilon}\bar{y} \to \mu(\bar{y}) = \mu(\bar{x}) + 1$ (d'après S_n) ; si $\bar{x} \neq \bar{y}$ et ou bien $\mu(\bar{x}) \neq 0$ ou bien $\mu(\bar{y}) \neq 0$, il existe $\bar{z}$, $\mu(\bar{z}) < \max(\mu(\bar{x}), \mu(\bar{y}))$ tel que $\bar{z}\bar{\varepsilon}\bar{x} \leftrightarrow \neg\, \bar{z}\bar{\varepsilon}\bar{y}$ (extensionnalité et S_n^ϕ). Ceci montre que $\mathfrak{M} = (E_0^c, ..., E_{n-1}^c, \bar{\varepsilon})$ satisfait C_n.

On notera que, si $(E_0', ..., E_{n-}', \bar{\varepsilon})$ satisfait C_n, il se peut que

$$(E_0', E_1' - E_0', ..., E_{n-1}' - E_{n-2}', \bar{\varepsilon})$$

ne satisfasse pas S_n : par exemple si $E_0' = \{a\}, E_1' = \{a, \{a\}\}$ $(a \neq \{a\})$,

$$E_2' = \{a, \{a\}, \{a, \{a\}\}\},$$

car $E'_1 - E'_0 = \{\{a\}\},\ E'_2 - E'_1 = \{\{a, \{a\}\}\},$

mais $\{a, \{a\}\}$ a des « éléments » et dans E'_0 et dans $E'_1 - E'_0$, en conflit avec l'axiome $\wedge x \wedge y \neg x \varepsilon y$ de S_3 où y est de type 2 et x de type 0.

b) L'application cherchée modifie la représentation des couples ordonnés de la théorie des ensembles de sorte que le couple devient de type pur et *simple*. On pose $\{x\}^0 = x$, et $\{x\}^{n+1} = \{\{x\}^n\}$. Si $\bar{x}_i \in E_i$ et $\bar{x}_j \in E_j$, on pose

$$\langle \bar{x}_i, \bar{x}_j \rangle = \{\{\bar{x}_i\}^{m-i+1}\ ,\ \{\{\bar{x}_i\}^{m-i}, \{\bar{x}_j\}^{m-j}\}\},$$

où $m = \max(i, j)$: le type de $\{\bar{x}_i\}^{m-i+1}$ est $m + 1$, de même pour $\{\{\bar{x}_j\}^{m-j}\}$, et par conséquent le type de $\langle \bar{x}_i, \bar{x}_j \rangle$ est $2 + m$. (Il est évident qu'il n'existe en général aucune injection de $E_i \times E_i$ dans E_{i+1} : si le cardinal de $E_i = 3$, card $E_i \times E_i = 9$ mais card $E_{i+1} \leqslant 8$.)

Cette application se définit dans le langage $\mathscr{L}^k_\varepsilon$, d'ailleurs uniformément pour toute k-réalisation de $\mathscr{L}^k_\varepsilon$ (c'est-à-dire au moyen de la même formule M_{ij}). Si x_i, x_j, x_k sont les variables de M_{ij}, l'unicité dans les deux directions

$$\wedge x_i \wedge x_j \wedge x_k \wedge x'_k([M_{ij}(x_i, x_j, x_k) \wedge M_{ij}(x_i, x_j, x'_k)] \to x_k = x'_k)$$

$$\wedge x_i \wedge x'_i \wedge x_j \wedge x'_j \wedge x_k([M_{ij}(x_i, x_j, x_k) \wedge \\ \wedge M_{ij}(x'_i, x'_j, x_k)] \to x_i = x'_i \wedge x_j = x'_j)$$

est conséquence de l'axiome d'extensionnalité (pour la formule M_{ij} considérée) ; seule la fonctionnalité

$$\wedge x_i \wedge x_j \vee x_k\ M_{ij}(x_i, x_j, x_k)$$

réclame l'axiome de couples.

L'extension aux p-uplets ordonnés est classique.

c) On définit les applications $\overline{M}_\sigma$ par récurrence sur la longueur de σ : pour $\sigma = 0$, on a l'identité, pour $\sigma = (\sigma_1, ..., \sigma_n)$ et $\bar{x} \in E_0$, on pose :

$$\overline{M}_\sigma \bar{x} = \{\langle \overline{M}_{\sigma_1} \bar{x}_1, ..., \overline{M}_{\sigma_n} \bar{x}_n \rangle ; (\bar{x}_1, ..., \bar{x}_n)\, \bar{\varepsilon}_\sigma\, \bar{x}\},$$

et on vérifie que les types des valeurs de $\overline{M}_\sigma$ sont bien ceux définis par la fonction N.

Comme ci-dessus *b*), l'unicité est conséquence de l'axiome d'extensionnalité. On n'effectue pas ici l'analyse explicite des conditions de clôture qui assurent la fonctionnalité.

6. On utilise les notations de l'exercice précédent. Pour tout entier $n \geqslant 0$ on définit $\mathfrak{C}^n_f(E)$ (l'ensemble des ensembles héréditairement finis sur E, du type cumulatif n) par récurrence sur n : $\mathfrak{C}^0_f(E) = E$; $\mathfrak{C}^{n+1}_f(E)$ est

la réunion de $\mathfrak{C}_f^n(E)$ et de l'ensemble de tous les sous-ensembles *finis* de $\mathfrak{C}_f^n(E)$.

Il est évident que la réalisation $\mathfrak{M}_f^n(E)$ de $\mathscr{L}_\varepsilon^n$ constituée par les ensembles de base $\mathfrak{C}_f^0(E), \ldots, \mathfrak{C}_f^n(E)$ et par la relation d'appartenance (restreinte à $\mathfrak{C}_f^n(E)$), satisfait C_{n+1} pourvu qu'aucun élément de $\mathfrak{C}_f^n(E)$ n'appartienne à aucun élément de E. De même si $\mathfrak{M}^n(E)$ est constituée par les ensembles de base $\mathfrak{C}^0(E), \ldots, \mathfrak{C}^n(E)$ où $\mathfrak{C}^0(E) = E$ et où

$$\mathfrak{C}^{m+1}(E) = \mathfrak{C}^m(E) \cup \mathfrak{P}(\mathfrak{C}^m(E)),$$

et par la relation d'appartenance restreinte à $\mathfrak{C}^n(E)$.

a) Montrer que, pour tout E satisfaisant : $\bar{x} \in \mathfrak{C}^n(E) \Rightarrow (\bar{y} \in E \Rightarrow \bar{x} \notin E)$, $\mathfrak{C}_f^n(E)$ est le plus petit (n)-modèle de C_{n+1} (à un isomorphisme près) contenant E comme ensemble de base de type 0 et vérifiant

$$\Lambda x \, \Lambda y \, \mathrm{V} z \, \Lambda u [u \varepsilon z \leftrightarrow (u \varepsilon x \vee u = y)]$$

où x, y, z, u sont respectivement de type i, j, k, l, avec $k = \max(i, j+1)$, $l < k \leqslant n$ (clôture par rapport à l'opération $x \cup \{ y \}$).

b) Montrer que les formules

$$\Lambda x \, \Lambda y \, \mathrm{V} z \, \Lambda u [u \varepsilon z \leftrightarrow (u \varepsilon x \wedge u \neq y)],$$

où x, y, z, u sont respectivement de type i, j, k, l et où

$$k + 1 = l = \max(i, j) \leqslant n,$$

ne sont pas des conséquences des axiomes figurant dans *a*) tandis qu'elles sont vérifiées dans $\mathfrak{M}_f^n$.

c) $\mathfrak{M}_f^2(E)$ et $\mathfrak{M}^2(E)$ seront écrites $\mathfrak{M}_f^2$, resp. $\mathfrak{M}^2$. Trouver trois formules P_1, P_2, P_3, à une seule variable libre (de type 1) telles que P_1 définisse, à la fois dans $\mathfrak{M}_f^2$ et dans $\mathfrak{M}^2$, l'ensemble $\mathscr{P}$ de tous les sous-ensembles finis à un nombre pair d'éléments, P_2 définit $\mathscr{P}$ dans $\mathfrak{M}_f^2$ mais non dans $\mathfrak{M}^2$ et P_3 définit $\mathscr{P}$ dans $\mathfrak{M}^2$, mais non dans $\mathfrak{M}_f^2$.

Solution.

a) Est évident par récurrence sur n en tenant compte du fait que, pour tout $\bar{x} \in \mathfrak{C}_f^{m+1}(E)$, $\bar{x} = \{ \bar{y}_1, \ldots, \bar{y}_s \}$, où $\bar{y}_i \in \mathfrak{C}_f^m(E)$ $(1 \leqslant i \leqslant s)$.

b) On considère un E infini, on prend $\{ E \} \cup \mathfrak{C}_f^1(E)$ pour l'ensemble de base du type 1, et $\mathfrak{C}_f^m(\{ E \} \cup \mathfrak{C}_f^1(E))$ pour l'ensemble de base du type $m + 1$. Les axiomes de (*a*) sont satisfaits, mais $E - \{ \bar{x} \}$ n'est élément de l'ensemble de base du type 1 pour aucun $\bar{x} \in E$.

c) Pour plus de clarté on ajoute au langage $\mathscr{L}_\varepsilon^3$ les symboles fonctionnels ϕ (à 0 variable, type 0), $\{ y \}$ (y de type 0, valeur de type 1),

$x \cup z$ et $x - z$ (x et z de type 1, valeur de type 1) qui sont définis et dans $\mathfrak{M}_f^2$ et dans $\mathfrak{M}^2$ par les axiomes suivants :

$$\Lambda x[x = \phi \leftrightarrow \Lambda y(\neg\, y\varepsilon x)]\,, \quad \Lambda x\, \Lambda y[x = \{\, y \,\} \leftrightarrow \Lambda u(u\varepsilon x \leftrightarrow u = y)]\,,$$

où u est de type 0,

$$\Lambda x\, \Lambda z\, \Lambda v[v = x \cup z \leftrightarrow \Lambda y(y\, \varepsilon\, v \leftrightarrow [y\varepsilon x \ \vee\ y\varepsilon z])]\,,$$

où v est de type 1,

et

$$\Lambda x\, \Lambda z\, \Lambda v[v\varepsilon x - z \leftrightarrow \Lambda y(y\varepsilon v \leftrightarrow [y\varepsilon x \wedge \neg\, y\varepsilon z])]\,.$$

D'après l'axiome d'extensionnalité, un modèle $\mathfrak{M}$ de C_3 ne peut être complété que d'une seule façon en un modèle $\mathfrak{M}^+$ du langage augmenté, d'où résulte l'élimination des nouveaux symboles par la méthode suivante (d'ailleurs applicable à tout symbole « explicitement défini ») : A toute formule A du langage augmenté on associe une formule A^- de $\mathscr{L}_\varepsilon^3$ telle que la réalisation de A dans $\mathfrak{M}^+$ est identique à la réalisation de A^- dans $\mathfrak{M}$. Il suffit de remplacer d'abord toute partie atomique $t\varepsilon t_1$, de A par une formule

$$\mathrm{V}u\, \mathrm{V}v(u = t \wedge v = t_1 \wedge u\varepsilon v)\,,$$

où u et v sont des variables ne figurant pas dans A de même type respectivement que t et t_1, et ensuite les équations ($u = t, v = t_1$) par leurs définitions (axiomes).

On prend pour P_1 la formule de $\mathscr{L}_\varepsilon^3$, dont la variable libre est y (de type 1), obtenue en éliminant les nouveaux symboles de la formule

$$y = \phi \vee \Lambda x[(y\varepsilon x \wedge \Lambda u\, \Lambda a\, \Lambda b[(a \neq b \wedge a\varepsilon u \wedge b\varepsilon u \wedge u\varepsilon x) \rightarrow \\ \rightarrow ((u - \{\, a \,\}) - \{\, b \,\})\, \varepsilon x]) \rightarrow \phi\varepsilon x]\,,$$

où x est de type 2, u de type 1, et a et b sont de type 0.

Soit A une formule close de $\mathscr{L}_\varepsilon^3$ qui est vraie dans $\mathfrak{M}^2$ et fausse dans $\mathfrak{M}_f^2$. Alors on pose :

$$P_2 = (\neg\, A \rightarrow P_1) \quad \text{et} \quad P_3 = (A \rightarrow P_1)\,.$$

(Puisque E est infini une telle A est, par ex., la formule de $\mathscr{L}_\varepsilon^3$ correspondant à

$$\mathrm{V}x(\phi\varepsilon x \wedge \Lambda u\, \Lambda a\, \Lambda b[(a \neq b \wedge \neg\, a\varepsilon u \wedge \neg\, b\varepsilon u \wedge u\varepsilon x) \rightarrow \\ \rightarrow ((u \cup \{\, a \,\}) \cup \{\, b \,\})\, \varepsilon x])\,.$$

On note en passant que la méthode dite de Dedekind pour définir $\mathscr{P}$ fournit aussi une P_3 :

$$\Lambda x[(\phi\varepsilon x \wedge \Lambda u\, \Lambda a\, \Lambda b[(a \neq b \wedge \neg\, a\varepsilon u \wedge \neg\, b\varepsilon u \wedge u\varepsilon x) \rightarrow \\ \rightarrow ((u \cup \{\, a \,\}) \cup \{\, b \,\})\, \varepsilon x]) \rightarrow y\varepsilon x\,]$$

7. On utilise les notations de l'exercice précédent ; en particulier, la variable x a le type 2, les variables y, u et w ont les types 1, et a et b ont le type 0. On écrira $y \cap u$ pour $y - (y - u)$.

a) Trouver des formules $N(y, u)$, $A(y, u, w)$, $S(y, u)$ de $\mathscr{L}_\varepsilon^3$ qui définissent respectivement dans $\mathfrak{M}_f^{(2)}$ et aussi dans $\mathfrak{M}^{(2)}$ les relations : (i) $\bar{y}$ et $\bar{u}$ sont deux ensembles finis de type 1 de même cardinal ($\bar{\bar{y}} = \bar{\bar{u}}$), (ii) $\bar{\bar{y}} + \bar{\bar{u}} = \bar{\bar{w}}$, (iii) $\bar{\bar{u}} = (\bar{\bar{y}})^2$.

b) En déduire une correspondance qui associe à toute formule F de l'Arithmétique du premier ordre (Chap. 3, Ex. 2) une formule F_ε de $\mathscr{L}_\varepsilon^3$ de telle façon que F est vraie dans le modèle standard si et seulement si F_ε est vraie dans $\mathfrak{M}_f^{(2)}$, et encore si et seulement si F_ε est vraie dans $\mathfrak{M}^{(2)}$.

Solution.

a) (i) On écrit y_1 pour $y - u$ et u_1 pour $u - y$; alors $y_1 \cap u_1 = \phi$. On prend pour formule N avec y', u' du type 1 :

$$\Lambda x[(\phi \varepsilon x \wedge$$
$$\wedge \Lambda y' \Lambda u' \Lambda a \, \mathsf{V} b[(y' \subset y_1 \wedge u' \subset u_1 \wedge y' \cup u' \varepsilon x \wedge a \varepsilon y_1 \wedge \neg\, a \varepsilon y')$$
$$\to (b \varepsilon u_1 \wedge \neg\, b \varepsilon u' \wedge y' \cup \{ a \} \cup u' \cup \{ b \} \varepsilon x)]) \to y_1 \cup u_1 \, \varepsilon x] .$$

On vérifie que $N(y, u)$ est satisfaite si et seulement si les ensembles $\bar{y}$ et $\bar{u}$ sont finis et si $\bar{\bar{y}} = \bar{\bar{u}}$.

(ii) On prend pour A :

$$\mathsf{V} y_1 \, \mathsf{V} u_1 [y_1 \cap u_1 = \phi \wedge N(y, y_1) \wedge N(u, u_1) \wedge N(w, y_1 \cup u_1)] .$$

On note que, pour $\bar{y}$ et $\bar{u}$ finis,

$$\mathsf{V} y_1 \, \mathsf{V} u_1 [y_1 \cap u_1 = \phi \wedge N(y, y_1) \wedge N(u, u_1)]$$

est toujours satisfaite (avec E infini).

(iii) On utilise le fait que $(m + 1)^2 = m^2 + 2m + 1$; on prend alors pour S :

$$\mathsf{V} y_1 \, \mathsf{V} u_1 [y_1 \cap u_1 = \phi \wedge$$
$$\wedge N(y, y_1) \wedge N(u, u_1) \wedge \Lambda x(\phi \varepsilon x \wedge \Lambda y' \Lambda u' \Lambda a$$
$$[(y' \subset y_1 \wedge u' \subset u_1 \wedge y' \cup u' \varepsilon x \wedge a \varepsilon y_1 \wedge \neg\, a \varepsilon y') \to$$
$$\to \mathsf{V} y'' \, \mathsf{V} u'' (A(y', y', y'') \wedge A(u' \cup \{ a \}, y'', u'') \wedge$$
$$\wedge u'' \subset u_1)]) \to y_1 \cup u_1 \, \varepsilon x] .$$

b) Partant de la formule F (close), on remplace les formules atomiques

$y.u = w$ d'abord par $(y + u)^2 - (y - u)^2 = w + w + w + w$ et ensuite par

$$\vee y'[(y' + u = y \vee y' + y = u) \wedge (y + u)^2 = y'^2 + w + w + w + w];$$

enfin on remplace $y = u$ par $N(y, u)$ (y et u étant des variables du type 1), $y + u = w$ par $A(y, u, w)$ et $y^2 = u$ par $S(y, u)$. La formule F' ainsi obtenue est vraie dans $E_f^{(2)}$ (pour E infini) si et seulement si F est vraie dans le modèle standard de l'Arithmétique. Si on restreint chaque variable du type 1, disons y, par la condition $N(y, y)$, on obtient la formule F_ε cherchée.

(Une définition formelle de « E est infini » est : $\wedge y \vee a(\neg\, a\varepsilon y)$ avec y de type 1 et a de type 0.)

Cet exercice réduit l'Arithmétique à la théorie des types (purs) 0,1 et 2, formulée en $\mathscr{L}_\varepsilon^3$: l'élimination des quantificateurs, Chap. 4, pour les anneaux de Boole exclut une telle réduction à la théorie des types 0 et 1 (formulée en $\mathscr{L}_\varepsilon^2$), cette théorie étant évidemment plongeable dans la théorie des anneaux de Boole atomiques.

---

6. DÉFINISSABILITÉ

Résumé

Dans ce chapitre il s'agit de certaines relations entre les formules d'un langage et leurs réalisations, c'est-à-dire les ensembles définis par ces formules dans les réalisations du langage.

Comme on a vu ci-dessus (par exemple, ex. 5, chap. 2, sur les formules prénexes purement universelles) la forme syntaxique d'une formule A peut entraîner des relations évidentes entre ses réalisations $\bar{A}_{\mathfrak{M}}$ dans les modèles $\mathfrak{M}$ différents ; du moins si les modèles considérés sont trivialement « comparables ». Inversement on se pose la question suivante : si les réalisations $\bar{A}_{\mathfrak{M}}$ satisfont les dites relations pour tous les modèles d'un ensemble $\mathscr{A}$ de formules, A est-elle (équivalente dans tout modèle de $\mathscr{A}$ à) une formule de la forme syntaxique en question ? Les deux cas principaux concernent d'une part les formules stables pour les extensions, d'autre part les formules invariantes pour les τ-réalisations des théories des types finis, introduites dans le chapitre précédent.

Pour comparer les modèles qui ne sont pas trivialement comparables on s'intéresse aux objets qui se « retrouvent » dans tous les modèles d'un ensemble $\mathscr{A}$ de formules, par exemple les rationnels dans tous les corps commutatifs de caractéristique 0. La notion nécessaire à une formulation précise est celle d'une structure *rigidement contenue* dans tous les modèles de $\mathscr{A}$, et le résultat principal établit que tout élément d'une telle structure est définissable au moyen de formules particulièrement simples.

Les deux derniers théorèmes caractérisent les sous-ensembles d'une telle partie commune qui sont définissables dans tout modèle de $\mathscr{A}$; deux notions de définissabilité sont traitées. Les caractérisations revêtent une forme spécialement simple s'il s'agit des modèles de la théorie des types (ex. 6). Ces deux notions de définissabilité permettent la généralisation de nombreux résultats classiques sur les ensembles « récursivement énumérables » d'axiomes à des ensembles quelconques d'axiomes. Cf. Kreisel [*Proc. Symp. Theory of Models*, 1963, Amsterdam (1965)], Mostowski [*Proc. Symp. Pure Mathematics*, **5**, 1961, AMS (1962)].

On considère des langages $\mathscr{L}$ égalitaires à p types de variables. $\bar{A}_{\mathfrak{M}}$ désigne la réalisation de la formule A dans la réalisation $\mathfrak{M}$ de $\mathscr{L}$. Si $\mathfrak{M}'$ est aussi une réalisation de $\mathscr{L}$ et si $\mathfrak{M}'$ est une extension de $\mathfrak{M}$, alors $\mathfrak{M} \cap \bar{A}_{\mathfrak{M}'}$ désigne, par abus de langage, la restriction de $\bar{A}_{\mathfrak{M}'}$ à $\mathfrak{M}$, c'est-à-dire

$$\bar{A}_{\mathfrak{M}'} \cap (E_1^{V_{\mathscr{L}}^{(1)}} \times \cdots \times E_p^{V_{\mathscr{L}}^{(p)}}),$$

où E_i est l'ensemble de base de $\mathfrak{M}$ de type i.

Soit $\mathscr{L}'$ un langage égalitaire disjoint de $\mathscr{L}$ et homotype à $\mathscr{L}$ (c'est-à-dire contenant aussi p types de variables et donné avec une bijection de $V_{\mathscr{L}}$, $R_{\mathscr{L}}$, $S_{\mathscr{L}}$, $F_{\mathscr{L}}$ sur $V_{\mathscr{L}'}$, $R_{\mathscr{L}'}$, $S_{\mathscr{L}'}$, $F_{\mathscr{L}'}$ qui conserve le type des variables, et le nombre de variables en argument ; l'image d'un symbole s de $\mathscr{L}$, par cette bijection, est noté s'. Ext $(\mathscr{L}, \mathscr{L}')$ désigne l'ensemble des formules suivantes de $\mathscr{L} \cup \mathscr{L}'$: $\bigwedge x_j \bigvee x'_j (x_j = x'_j)$ pour $1 \leqslant j \leqslant p$, où x_j est une variable de type j,

$$\bigwedge x_1 \dots \bigwedge x_n \bigwedge x'_1 \dots \bigwedge x'_n [(x_1 = x'_1 \wedge \cdots \wedge x_n = x'_n) \rightarrow (Rx_1 \dots x_n \leftrightarrow R' x'_1 \dots x'_n)]$$

pour tout symbole relationnel R de $\mathscr{L}$,

$$\bigwedge x_1 \dots \bigwedge x_n \bigwedge x'_1 \dots \bigwedge x'_n [(x_1 = x'_1 \wedge \cdots \wedge x_n = x'_n) \rightarrow fx_1 \dots x_n = f'x'_1 \dots x'_n]$$

pour tout symbole fonctionnel de $\mathscr{L}$, et pour toute suite $x_1, \dots, x_n$ admise pour R, resp. f.

Lemme. — *La réalisation $\mathfrak{M}'$ de $\mathscr{L}'$ est une extension de la réalisation $\mathfrak{M}$ de $\mathscr{L}$ si et seulement si la somme $\mathfrak{M} \oplus \mathfrak{M}'$ est une réalisation de $\mathscr{L} \cup \mathscr{L}'$ qui satisfait* Ext $(\mathscr{L}, \mathscr{L}')$.

La formule A de $\mathscr{L}$ est dite *$(\mathscr{U}, \mathscr{A})$-invariante* si pour tout modèle $\mathfrak{M}$ de $\mathscr{U}$ et pour tout couple de modèles $\mathfrak{M}'$, $\mathfrak{M}''$ de $\mathscr{A}$ tels que $\mathfrak{M}'$ et $\mathfrak{M}''$ soient des extensions de $\mathfrak{M}$, $\mathfrak{M} \cap \overline{A}_{\mathfrak{M}'} = \mathfrak{M} \cap \overline{A}_{\mathfrak{M}''}$. (Puisqu'on ne suppose pas $\mathfrak{M}$ modèle de $\mathscr{A}$, en général $\overline{A}_{\mathfrak{M}} \neq \mathfrak{M} \cap \overline{A}_{\mathfrak{M}'}$; voir l'exercice 1 pour l'utilité de la notion de $(\mathscr{U}, \mathscr{A})$-invariance). Soient $x_1, \dots, x_n$ les variables libres de A.

Théorème 1. — (*Théorème d'invariance*). — *Si A est $(\mathscr{U}, \mathscr{A})$-invariante il existe une formule B telle que* :

$$\mathscr{A}' \cup \mathscr{U} \cup \text{Ext}(\mathscr{L}, \mathscr{L}') \vdash$$
$$\vdash \bigwedge x_1 \dots \bigwedge x_n \bigwedge x'_1 \dots \bigwedge x'_n \; [(x_1 = x'_1 \wedge \cdots \wedge x_n = x'_n) \rightarrow (A' \leftrightarrow B)] \, .$$

Démonstration. — On ajoute les constantes $a_1, \dots, a_n$ (a_i du même type que x_i) et on introduit le langage $\mathscr{L}''$ homotype à $\mathscr{L}$ et disjoint de $\mathscr{L}$ et de $\mathscr{L}'$. Puisque A est $(\mathscr{U}, \mathscr{A})$-invariante :

$$\mathscr{A}' \cup \mathscr{A}'' \cup \mathscr{U} \cup \text{Ext}(\mathscr{L}, \mathscr{L}') \cup \text{Ext}(\mathscr{L}, \mathscr{L}'')$$
$$\cup \{ A', \neg A'', a_1 = a'_1 \wedge \cdots \wedge a_n = a'_n, a_1 = a''_1 \wedge \cdots \wedge a_n = a''_n \}$$

n'a pas de modèle. En séparant les langages $\mathscr{L}'$ et $\mathscr{L}''$, c'est-à-dire les ensembles

$$\mathscr{A}' \cup \mathscr{U} \cup \{ \text{Ext}(\mathscr{L}, \mathscr{L}') \} \cup \{ A', a_1 = a'_1 \wedge \cdots \wedge a_n = a'_n \}$$

et

$$\mathscr{A}'' \cup \mathscr{U} \cup \{ \text{Ext}(\mathscr{L}, \mathscr{L}'') \} \cup \{ \neg A'', a_1 = a''_1 \wedge \cdots \wedge a_n = a''_n \} ,$$

le lemme d'interpolation (chapitre 5) avec égalité montre qu'il existe une formule Y de $\mathcal{L} \cup \{ a_1, ..., a_n \}$ telle que :

$$\mathcal{A}' \cup \mathcal{U} \cup \{ \text{Ext}(\mathcal{L}, \mathcal{L}') \} \cup \{ a_1 = a'_1 \wedge \cdots \wedge a_n = a'_n \} \vdash A' \to Y$$

et :

$$\mathcal{A}'' \cup \mathcal{U} \cup \{ \text{Ext}(\mathcal{L}, \mathcal{L}'') \} \cup \{ a_1 = a''_1 \wedge \cdots \wedge a_n = a''_n \} \vdash \neg A'' \to \neg Y.$$

En remplaçant a_i par x_i dans $Y (1 \leqslant i \leqslant n)$, on obtient une formule B telle que si on identifie les langages $\mathcal{L}'$ et $\mathcal{L}''$:

$$\mathcal{A}' \cup \mathcal{U} \cup \text{Ext}(\mathcal{L}, \mathcal{L}') \vdash \bigwedge x_1, ..., \bigwedge x_n \bigwedge x'_1, ..., \bigwedge x'_n$$
$$[(x_1 = x'_1 \wedge \cdots \wedge x_n = x'_n) \to (A' \leftrightarrow B)].$$

La formule A du langage $\mathcal{L}$ est dite *existentielle* (*universelle*) si A est prénexe et si tous ses quantificateurs sont existentiels (universels).

La formule A est dite *$\mathcal{A}$-stable pour les extensions* si, pour tout couple $\mathfrak{M}$, $\mathfrak{M}'$ de modèles de $\mathcal{A}$ tels que $\mathfrak{M}'$ est une extension de $\mathfrak{M}$, on a $\overline{A}_{\mathfrak{M}'} \cap \mathfrak{M} \supset \overline{A}_{\mathfrak{M}}$; en particulier, si A est une formule close vraie dans $\mathfrak{M}$, alors A est aussi vraie dans $\mathfrak{M}'$.

A est dite *$\mathcal{A}$-stable pour les restrictions* si $\neg A$ est $\mathcal{A}$-stable pour les extensions.

Il est évident que, pour tout $\mathcal{A}$, une formule existentielle est $\mathcal{A}$-stable pour les extensions, et une formule universelle est $\mathcal{A}$-stable pour les restrictions.

THÉORÈME 2. — *Soit $\mathcal{A}$ un ensemble de formules closes de $\mathcal{L}$ et soient A et B deux formules de $\mathcal{L}$ telles que, pour tout couple $\mathfrak{M}$, $\mathfrak{M}'$ de modèles de $\mathcal{A}$ avec $\mathfrak{M}'$ extension de $\mathfrak{M}$, on ait $\overline{A}_{\mathfrak{M}'} \cap \mathfrak{M} \subset \overline{B}_{\mathfrak{M}}$. Alors il existe une formule universelle U de $\mathcal{L}$ telle que*

$$\mathcal{A} \vdash (A \to U) \text{ et } \mathcal{A} \vdash (U \to B).$$

Démonstration (voir aussi Ex. 2).

Soit $\mathcal{L}'$ le langage $\mathcal{L}$ augmenté par un ensemble V'_C de (nouvelles) constantes d'individu, V'_C ayant la cardinalité de $\mathcal{L}$. Soient A_1, B_1 deux formules de $\mathcal{L}'$ obtenues en remplaçant chacune des variables libres de A et de B par un élément de V'_C ; soit V_1 l'ensemble, éventuellement vide, de ces constantes. Soit $\mathcal{U}$ l'ensemble des formules universelles de $\mathcal{L} \cup V_1$, qui sont conséquences de $\mathcal{A} \cup \{ A_1 \}$.

Il suffit de démontrer que $\mathcal{A} \cup \mathcal{U} \cup \{ \neg B_1 \}$ n'a pas de modèle ; car dans ce cas, d'après le théorème de finitude il existe un sous-ensemble fini $\mathcal{U}_F$ de $\mathcal{U}$ tel que $\mathcal{A} \cup \mathcal{U}_F \vdash B_1$, et par conséquent $\mathcal{A} \vdash U_F \to B_1$, où U_F désigne la conjonction des formules de $\mathcal{U}_F$. Or U_F est équivalent à une formule universelle. D'autre part, d'après la définition de l'ensemble $\mathcal{U}$, $\mathcal{A} \vdash (A_1 \to U_F)$.

Supposons que $\mathcal{A} \cup \mathcal{U} \cup \{ \neg B_1 \}$ ait un modèle $\mathfrak{M}$ et soit $\mathcal{D}'$ le diagramme

de $\mathfrak{M}$ écrit avec les symboles V'_C. Alors tout modèle $\mathfrak{M}'$ de $\mathscr{A} \cup \mathscr{D}'$ est extension de $\mathfrak{M}$ à un isomorphisme près. Puisque B_1 n'est pas satisfaite dans $\mathfrak{M}$, *d'après l'hypothèse du théorème, A_1 n'est pas satisfaite dans $\mathfrak{M}'$*, et par conséquent $\mathscr{A} \cup \mathscr{D}' \vdash \neg A_1$. Il existe donc un sous-ensemble fini $\mathscr{D}'_F$, dont la conjonction sera notée D'_F, tel que $\mathscr{A} \cup \mathscr{D}'_F \vdash \neg A_1$ et aussi $\mathscr{A} \vdash (A_1 \to \neg D'_F)$.

Soit D''_F une formule obtenue en remplaçant les constantes de $V'_C - V_1$ qui figurent dans D'_F par des variables de $\mathscr{L}$ prises parmi $y_1, ..., y_n$. Alors la formule universelle $\wedge y_1 ... \wedge y_n \neg D''_F$ de $\mathscr{L} \cup V_1$ est conséquence de $\mathscr{A} \cup \{ A_1 \}$ et donc $\in \mathscr{U}$. Ceci montre que $\mathscr{A} \cup \mathscr{U} \cup \mathscr{D}'$ n'a pas de modèle parce que

$$(\wedge y_1 ... \wedge y_n \neg D''_F) \to \neg D'_F ,$$

et par conséquent $\mathscr{A} \cup \mathscr{U} \cup \mathscr{D}' \cup \{ \neg B_1 \}$ n'a pas non plus de modèle. Puisque $\mathfrak{M}$ est arbitraire, $\mathscr{A} \cup \mathscr{U} \cup \{ \neg B_1 \}$ est contradictoire.

COROLLAIRE. — *Si la formule C est $\mathscr{A}$-stable pour les extensions il existe une formule existentielle E telle que $\mathscr{A} \vdash (C \leftrightarrow E)$.*

Démonstration. — Si C est $\mathscr{A}$-stable, $\neg C$ satisfait les hypothèses du théorème 2 en posant $A = B = \neg C$.

C. q. f. d.

Dans les exercices 3-5 on considérera les notions d'invariance et de stabilité adaptées aux τ-réalisations au sens du chapitre 5.

Les théorèmes qui suivent concernent des classes de modèles qui ne sont pas « comparables ».

La réalisation $\mathfrak{M}$ du langage $\mathscr{L}$ est dite *rigidement contenue* dans $\mathfrak{M}'$ s'il existe une *seule* application φ' des ensembles de base $E_1, ..., E_p$ de $\mathfrak{M}$ dans $E'_1 \cup \cdots \cup E'_p$ telle que $\varphi'(E_i) \subset E'_i$ $(1 \leqslant i \leqslant p)$; pour toute constante c de $\mathscr{L}$, $\varphi(\bar{c}) = \bar{c}'$; pour tout symbole relationnel R, l'image de $\bar{R}$ par φ' est induite par $\bar{R}'(\bar{c}', \bar{R}'$ désignant respectivement les réalisations de c, R dans $\mathfrak{M}'$).

$\mathfrak{M}$ est dite rigidement contenue dans la *classe* des modèles d'un ensemble $\mathscr{A}$ de formules de $\mathscr{L}$ si $\mathfrak{M}$ est rigidement contenue dans tout modèle de $\mathscr{A}$. *On ne suppose pas que $\mathfrak{M}$ soit modèle de $\mathscr{A}$.*

Une formule A, à une seule variable libre x, est appelée une *définition dans $\mathfrak{M}$ de l'élément a* $(a \in E_i)$ si a est le seul élément qui satisfait A, ou encore si

$$\bar{A} = \left\{ \delta \in \prod_{i=1}^{n} E_i^{V_{\mathscr{L} i}} \ ; \ \delta(x) = a \right\} ;$$

par abus de langage on dira : $\bar{A} = \{ a \}$.

THÉORÈME 3. — *Si $\mathfrak{M}$ est rigidement contenue dans la classe des modèles de $\mathscr{A}$ alors, pour tout élément a de l'ensemble de base M de $\mathfrak{M}$, il existe une formule existentielle A_a de $\mathscr{L}$ telle que :*

(i) *A_a définit l'élément a dans $\mathfrak{M}$ et dans tout modèle $\mathfrak{M}'$ de $\mathscr{A}$, A_a définit $\varphi'(a)$;*

(ii) *pour tout symbole relationnel R de $\mathscr{L}$ à n variables et pour tout n-uplet* $(a_1, ..., a_n)$ *d'individus de* $\mathfrak{M}$:

$$(a_1, ..., a_n) \in \overline{R} \Leftrightarrow \mathscr{A} \vdash \wedge x_1 ... \wedge x_n[(A_{a_1}x_1 \wedge \cdots \wedge A_{a_n}x_n) \rightarrow R(x_1 ... x_n)]$$

$$(a_1, ..., a_n) \notin \overline{R} \Leftrightarrow \mathscr{A} \vdash \wedge x_1 ... \wedge x_n[(A_{a_1}x_1 \wedge \cdots \wedge A_{a_n}x_n) \rightarrow \neg R(x_1 ... x_n)] .$$

Démonstration. — Ajoutons au langage $\mathscr{L}$ les constantes c'_a, c''_a $(a \in M)$ distinctes deux à deux et non dans $C_{\mathscr{L}}$. Soient D', D'' les diagrammes de $\mathfrak{M}$ pour ces constantes. Puisque dans tout modèle $\mathfrak{M}'$, resp. $\mathfrak{M}''$, de $\mathscr{A}$ il y a une seule façon de satisfaire D', resp. D'' (rigidité), à savoir $\overline{c}'_a = \varphi' a$ et $\overline{c}''_a = \varphi'' a$ pour tout a, alors

$$\mathscr{A} \cup D' \cup D'' \vdash c'_a = c''_a .$$

D'après le théorème de finitude il existe deux sous-ensembles finis D'_1, D''_2 tels que

$$\mathscr{A} \cup D'_1 \cup D''_2 \vdash c'_a = c''_a .$$

Soit B_a la conjonction des formules obtenues en remplaçant les constantes de D', autres que c'_a par x_i $(1 \leqslant i \leqslant h)$, toutes les constantes de D''_2 par y_j $(1 \leqslant j \leqslant k)$ et c'_a par x. On pose $A_a = \vee x_1 ... \vee x_h \vee y_1 ... \vee y_k B_a$. On a $\vee x A_a x$ parce que dans tout modèle $\mathfrak{M}'$ de $\mathscr{A}$, $D'_1 \cup D''_2$ est satisfait en posant $\overline{c}'_b = \overline{c}''_b = \varphi' b$ pour tout b. L'unicité est conséquence de

$$\mathscr{A} \cup D'_1 \cup D''_2 \vdash c'_a = c''_a ,$$

et (i) est ainsi démontré. Le (ii) (saturation) est satisfait parce que $\varphi'(\overline{R})$ est par hypothèse la réalisation de R dans $\mathfrak{M}'$.

COROLLAIRE. — *Sous les conditions du théorème* 3, *si on ajoute à* $\mathscr{L}$ *les constantes* c_a *pour tout* $a \in M$, *tout modèle* $\mathfrak{M}'$ *de* $\mathscr{A}$ *peut être complété d'une seule façon en un modèle de* $\mathscr{A} \cup \mathscr{A}_1$, *où*

$$\mathscr{A}_1 = \{ \wedge x(A_a x \leftrightarrow x = c_a) \, ; \, a \in M \} ;$$

dans ce modèle $\overline{c}_a = \varphi' a$. *En particulier,* $\mathscr{A} \cup \mathscr{A}_1 \vdash c_a \neq c_b$ *pour tout couple* (a, b) *avec a distinct de b.*

Soit $\mathscr{L}$ un langage à k types d'objets, contenant un ensemble infini **C** de constantes c (de type i, $i \leqslant k$). On appelle **C**-*réalisation* de $\mathscr{L}$ une réalisation égalitaire dans laquelle $\overline{c} = c$ pour tout $c \in$ **C**. Un sous-ensemble X de **C** est dit *définissable dans une* **C**-*réalisation* $\mathfrak{M}$ de $\mathscr{L}$ s'il existe une formule $A(x, x_1, ..., x_n)$, où x est de type i, et des éléments $a_1, ..., a_n$ de $\mathfrak{M}$ de mêmes types respectifs que $x_1, ..., x_n$, tels que

$$X = \{ a : a \in \mathfrak{M} \, , \, a \text{ est de type } i, \; (a, a_1, ..., a_n) \in \overline{A} \}$$

($\overline{A}$ étant la valeur prise par A dans $\mathfrak{M}$).

Il est évident que si X est fini, soit $X = \{ c_1, ..., c_m \}$, alors X est définissable dans toute **C**-réalisation par la formule $x = c_1 \vee \cdots \vee x = c_m$.

Théorème 4. — *Si $\mathscr{A}$ est un ensemble de formules closes de $\mathscr{L}$ qui a un* **C**-*modèle et si X est définissable dans tous les* **C**-*modèles de $\mathscr{A}$, X est un ensemble fini.*

Démonstration. — Remarquons d'abord qu'une **C**-réalisation est, à un isomorphisme près, une réalisation quelconque dans laquelle les valeurs prises par deux éléments distincts de **C** sont distinctes. Nous supposons donc que $\mathscr{A}$ contient toutes les formules $c \neq c'$ pour tous les couples (c, c') d'éléments distincts de **C**.

On construit le langage $\mathscr{L}_\Delta$ et l'ensemble de formules Ω comme il a été expliqué chapitre 5. Le cardinal de l'ensemble de formules de Ω ayant une seule variable libre (de type i) étant égal à card $\mathscr{L}_\Delta$, on énumère cet ensemble en le mettant sous la forme $\{ A_j\, x : j < \text{card}\, \mathscr{L}_\Delta \}$

Soit $\mathscr{A}_0^+ = \mathscr{A} \cup \Omega$, et pour $j > 0$:

1° $\mathscr{A}_j^+ = \bigcup_{h<j} \mathscr{A}_h^+ \cup \{ \mathsf{V}x\, A_j x \} \cup \{ \varepsilon A_j x \neq c : c \in \mathbf{C} \}$ si cet $\mathscr{A}_j^+$ est consistant

2° $\mathscr{A}_j^+ = \bigcup_{h<j} \mathscr{A}_h^+$ si le 1° ne s'applique pas.

Dans le cas 2°, d'après le théorème de finitude, il existe un ensemble fini $\{ c_1, ..., c_{n_j} \}$ tel que

$$\bigcup_{h<j} \mathscr{A}_h^+ \vdash \Lambda x[A_j x \to (x = c_1 \vee \cdots \vee x = c_{n_j})]\,.$$

D'après le corollaire du théorème de finitude, $\{ \bigcup \mathscr{A}_j^+ : j < \text{card}\, \mathscr{L}_\Delta \}$ a un modèle canonique (si $\mathscr{A}$ a un modèle). Dans ce modèle, si j satisfait le 1°, alors $\overline{A}_j \not\subset \mathbf{C}$, et par conséquent $\overline{A}_j \neq X$; si j satisfait le 2°, $\overline{A}_j$ est fini. Donc, si X est définissable dans un tel modèle, X est fini. C. q. f. d.

Un sous-ensemble X de **C** est dit définissable *sur* **C** dans une **C**-réalisation $\mathfrak{M}$ de $\mathscr{L}$ s'il existe une formule $A(x, x_1, ..., x_n)$, où x est de type i, et des éléments $a_1, ..., a_n$ de $\mathfrak{M}$ de mêmes types respectifs que $x_1, ..., x_n$ tels que

$$X = \{ c : c \in \mathbf{C}, (c, a_1, ..., a_n) \in \overline{A} \}\,.$$

Il est évident que X est définissable *sur* **C** dans toute **C**-réalisation d'un ensemble $\mathscr{A}$ de formules s'il existe une formule Ax, à une seule variable libre, telle que, pour tout $c \in \mathbf{C}$

$$c \in X \Leftrightarrow \mathscr{A} \vdash Ac \qquad \text{et} \qquad c \notin X \Leftrightarrow \mathscr{A} \vdash \neg Ac\,.$$

La réciproque est fausse (voir exercice 9) ; cependant on a la proposition suivante (voir exercice 8 pour une simplification dans le cas des langages dénombrables) :

THÉORÈME 5. — *Soit* $\mathscr{A}$ *un ensemble de formules closes de* $\mathscr{L}$ *ayant un* **C**-*modèle et soient* $b_1^*, b_2^*, \ldots$ *des constantes non dans* $\mathscr{L}$. *Si* $X \subset \mathbf{C}$ *est définissable sur* **C** *dans tous les* **C**-*modèles de* $\mathscr{A}$, *il existe une formule* $A(x, x_1, \ldots, x_n)$ *de* $\mathscr{L}$ *et une famille de formules* $F_j(x_1, \ldots, x_n)$ $(j < \lambda)$ *de* $\mathscr{L}$ *telles que* :

$$\text{card}\,\lambda < \text{card}\,\mathscr{L} \text{ et card}\,\lambda \leqslant \text{card}\,\mathbf{C}\,,$$

$\mathscr{A} \cup \{ F_j(b_1^*, \ldots, b_n^*) : j < \lambda \}$ *a un modèle et pour tout* $c \in \mathbf{C}$:

$c \in X \Leftrightarrow$ *il existe* $j < \lambda$: $\mathscr{A} \vdash \Lambda x_1 \ldots \Lambda x_n [F_j(x_1, \ldots, x_n) \rightarrow A(c, x_1, \ldots, x_n)]$.

$c \notin X \Leftrightarrow$ *il existe* $j < \lambda$: $\mathscr{A} \vdash \Lambda x_1 \ldots \Lambda x_n [F_j(x_1, \ldots, x_n) \rightarrow \neg A(c, x_1, \ldots, x_n)]$

(Ce théorème se déduit aussi d'un théorème plus général sur les formules infinies, donné dans le prochain chapitre.)

On va montrer que, si la conclusion de ce théorème n'est pas satisfaite, alors X n'est pas définissable dans une certaine classe de modèles canoniques.

Soit $A_j\,x$ une énumération, éventuellement transfinie, de toutes les formules de $\mathscr{L}_\Delta$ à une seule variable libre (de type i). Toute formule étant finie et card $\mathscr{L}_\Delta$ étant infini, l'ensemble de ces formules a le même cardinal que $\mathscr{L}_\Delta$. On suppose donc $j <$ card $\mathscr{L}_\Delta$.

Soit $\mathscr{A}_0^+ = \mathscr{A} \cup \Omega$. Pour $j > 0$,

Cas 1 : Pour tout $k \leqslant j$, $\{ A_k c : c \in \mathbf{C},\ c \in X \} \cup \{ \neg A_k c : c \in \mathbf{C},\ c \notin X \}$ n'est pas conséquence de

$$\bigcup_{h<k} \mathscr{A}_h^+ ;$$

a) $\mathscr{A}_j^+ = \bigcup_{h<j} \mathscr{A}_h^+ \cup \{ \neg A_j c_j \}$ s'il existe un $c \in X$ tel que $A_j c$ n'est pas conséquence de $\bigcup_{h<j} \mathscr{A}_h^+$, soit $c = c_j$.

b) $\mathscr{A}_j^+ = \bigcup_{h<j} \mathscr{A}_h^+ \cup \{ A_j c_j \}$ si *a*) ne s'applique pas ; il existe donc alors un $c \notin X$ tel que $\neg A_j c$ n'est pas conséquence de

$$\bigcup_{h<j} \mathscr{A}_h^+ .$$

Cas 2 : Le cas 1 ne s'applique pas. On pose

$$\mathscr{A}_j^+ = \bigcup_{h<j} \mathscr{A}_h^+ .$$

D'après le corollaire au théorème de finitude, $\bigcup_j \mathscr{A}_j^+$ a un modèle canonique $\mathfrak{M}$. Si le cas 1 s'applique, $X \neq \bar{A}_j \cap \mathbf{C}$; par conséquent, s'il s'applique pour tout j, X n'est pas définissable *sur* **C** dans $\mathfrak{M}$, tout élément de $\mathfrak{M}$ ayant un nom dans $\mathscr{L}_\Delta$. Donc il y a un λ ($\lambda <$ card $\mathscr{L}$) tel que

$$\{ A_\lambda c : c \in \mathbf{C}, c \in X \} \cup \{ \neg A_\lambda c : c \in \mathbf{C}, c \notin X \}$$

soit conséquence de

$$\mathscr{A} \cup \{ A'_j c_j : j < \lambda \},$$

où $A'_j = \neg A_j$ si 1 *a*) s'applique, et $A'_j = A_j$ si 1 *b*) s'applique.

Pour tout $c \in \mathbf{C}$, $\{ A_\lambda c : c \in X \} \cup \{ \neg A_\lambda c : c \notin X \}$ est donc conséquence de

$$\mathscr{A} \cup \{ A'_j c_j : j \in I_c \}$$

pour un certain sous-ensemble fini I_c d'ordinaux $< \lambda$. Soient $b_1^*, \ldots, b_n^*$ les éléments de Δ qui figurent dans A_λ et $a_1, \ldots, a_m$ ceux qui figurent dans $\{ A'_j c_j : j \in I_c \}$. On a (Lemme 6, Chap. 5)

$$\{ A'_j c_j : j \in I_c \} \cup \mathscr{A} \cup (\theta_{a_1} \wedge \cdots \wedge \theta_{a_m} \wedge \theta_{b_1^*} \wedge \cdots \wedge \theta_{b_n^*}) \vdash$$

$$\vdash \{ A_\lambda c : c \in X \} \cup \{ \neg A_\lambda c : c \notin X \}$$

et on pose

$$F_c(b_1^*, \ldots, b_n^*) = \theta_{a_1} \wedge \cdots \wedge \theta_{a_m} \wedge \theta_{b_1^*} \wedge \cdots \wedge \theta_{b_n} \wedge A^c,$$

où A^c est la conjonction des $A'_j c_j$ ($j \in I_c$).

EXERCICES

1. On utilise les notations du Théorème d'invariance. Démontrer les résultats suivants :

a) Si A est $(\mathscr{U}, \mathscr{A})$-invariante et si toute conséquence (prénexe) universelle de $\mathscr{A}$ est aussi conséquence de $\mathscr{U}$, alors les formules B et $\neg B$ (théorème d'invariance) sont toutes deux $\mathscr{U}$-stables.

b) Si les conditions de *a*) sont satisfaites et si $\mathscr{U}$ est un ensemble de formules purement universelles alors il existe une formule C sans quantificateurs telle que $\mathscr{U} \vdash (B \leftrightarrow C)$. (Voir *e*).)

c) Si $\mathscr{U}$ est l'ensemble des conséquences universelles de $\mathscr{A}$ et si toute formule existentielle est $(\mathscr{U}, \mathscr{A})$-invariante, alors pour toute formule A il existe une formule B sans quantificateur telle que $\mathscr{A} \vdash (A \leftrightarrow B)$.

d) Déduire de *c*) les critères « algébriques » suivants d'élimination des quantificateurs : (i) pour les corps algébriquement clos : s'il existe un corps algébriquement clos contenant le corps commutatif C et dans lequel une formule existentielle F est vraie, alors F est vraie dans la clôture algébrique de C ; (ii) de même pour les corps réels fermés, C étant un corps ordonné.

e) Trouver un contre-exemple à l'énoncé *b*) si on supprime la condition que $\mathscr{U}$ ne contienne que des formules universelles.

Solution.

a) D'après le théorème de plongement, tout modèle de $\mathscr{U}$ peut être plongé dans un modèle de $\mathscr{A}$. Soient donc $\mathfrak{M}$ et $\mathfrak{M}_1$ deux modèles de $\mathscr{U}$, $\mathfrak{M}_1$ extension de $\mathfrak{M}$, et soit $\mathfrak{M}'$ une extension de $\mathfrak{M}_1$, qui est un modèle de $\mathscr{A}$. Si B est vraie dans $\mathfrak{M}$, A est vraie dans $\mathfrak{M}'$, $\mathfrak{M}'$ étant extension de $\mathfrak{M}$ et modèle de $\mathscr{A}$. Par conséquent, B est vraie dans $\mathfrak{M}_1$, $\mathfrak{M}'$ étant aussi extension de $\mathfrak{M}_1$. De même pour $\neg B$.

b) D'après le théorème 2, il existe deux formules existentielles C_1 et C_2 telles que $\mathscr{U} \vdash (B \leftrightarrow C_1)$ et $\mathscr{U} \vdash (\neg B \leftrightarrow C_2)$, B et $\neg B$ étant $\mathscr{U}$-stables. Par conséquent (théorème de finitude), il y a un sous-ensemble fini $\mathscr{U}_1$ de $\mathscr{U}$ tel que $\mathscr{U}_1 \vdash (C_1 \leftrightarrow \neg C_2)$; appliquer alors l'exercice 3 *c*) chapitre 5.

c) Puisque $\mathscr{A} \vdash \mathscr{U}$, on a d'après *b*) : $\mathscr{A} \vdash (B \leftrightarrow C)$. Or pour l'élimination des quantificateurs il suffit que toute formule existentielle admette l'élimination des quantificateurs (Chap. 4).

d) (i) Soit $\mathscr{A}$ l'ensemble des axiomes des corps algébriquement clos (Chap. 4) et $\mathscr{U}$ l'ensemble des axiomes des corps commutatifs. On a évidemment $\mathscr{A} \vdash \mathscr{U}$, et on sait que tout corps commutatif peut être plongé dans un corps algébriquement clos (sa clôture algébrique). Par conséquent, les hypothèses de *c*) sont satisfaites. (ii) $\mathscr{U}$ est l'ensemble des axiomes des corps ordonnés. (Si au lieu de $\mathscr{U}$ on choisit les axiomes $\mathscr{U}'$ des corps réels, qui sont les corps ordonnables, le *c*) s'applique mais le critère n'est pas utile parce qu'il y a des formules existentielles qui ne sont pas $(\mathscr{U}', \mathscr{A})$-invariantes.)

e) On considère le langage $\mathscr{L}$ de l'exercice 2, chapitre 4 et les axiomes $\mathscr{U} = a), b), c), e)$, p. 51 : bien que $\mathscr{U} \vdash (2 \mid x) \vee (2 \mid x+1)$ et que $2 \mid x$ soit purement existentielle, $2 \mid x$ n'est équivalente à aucune formule sans quantificateurs de $\mathscr{L}$.

2. On utilisera les notations du théorème 2.
Démontrer le théorème 2 à l'aide du lemme d'interpolation (Chap. 5).

Solution. — Soit $\mathrm{Ext}_1(\mathscr{L}, \mathscr{L}')$ la conjonction des formules (universelles)

$$\wedge x_1 \ldots \wedge x_n \wedge x'_1 \ldots \wedge x'_n[(x_1 = x'_1 \wedge \cdots \wedge x_n = x'_n) \rightarrow \rightarrow (Rx_1 \ldots x_n \leftrightarrow R'x'_1 \ldots x'_n)]$$

et

$$\wedge x_1 \ldots \wedge x_n \wedge x'_1 \ldots \wedge x'_n[(x_1 = x'_1 \wedge \cdots \wedge x_n = x'_n) \rightarrow \rightarrow fx_1 \ldots x_n = f'x'_1 \ldots x'_n]$$

pour tout symbole relationnel R et pour tout symbole fonctionnel f de $\mathscr{L}$ et pour toute suite $x_1, \ldots, x_n$ admise pour R, respectivement f.

Si A et B contiennent moins de m variables libres, $\mathscr{L}_1$ est le langage $\mathscr{L}$ augmenté par des constantes (nouvelles) d'individu $a_r (r < m)$, et $\mathscr{L}'_1$ est $\mathscr{L}'$ augmenté par a'_r $(r < m)$. A_1 et B_1 sont des formules de $\mathscr{L}_1$ obtenues en remplaçant toutes les variables libres de A, resp. B, par des nouvelles constantes. On désigne par $\text{Ext}_1(\mathscr{L}_1, \mathscr{L}'_1)$ la formule

$$\text{Ext}_1(\mathscr{L}, \mathscr{L}') \wedge \cdots \wedge a'_r = a_r \wedge \cdots (r < m).$$

D'après l'hypothèse du théorème 2

$$\mathscr{A} \cup \mathscr{A}' \cup \{ \Lambda y_1 \mathsf{V} y'_1(y'_1 = y_1) \wedge \cdots \wedge \Lambda y_p \mathsf{V} y'_p(y'_p = y_p) \wedge \wedge \text{Ext}_1(\mathscr{L}_1, \mathscr{L}'_1) \wedge A'_1 \} \vdash B_1$$

où y_j $(1 \leqslant j \leqslant p)$ est une variable de $\mathscr{L}$ du type j.

D'après le théorème de finitude, il existe des conjonctions A_F, A'_F de formules de $\mathscr{A}$, resp. $\mathscr{A}'$, telles que

$$A'_F \wedge A'_1 \wedge \Lambda y_1 \mathsf{V} y'_1 (y'_1 = y_1) \wedge \cdots \wedge \Lambda y_p \mathsf{V} y_p (y'_p = y_p) \wedge \wedge \text{Ext}_1(\mathscr{L}_1, \mathscr{L}'_1) \vdash (A_F \to B_1).$$

Par conséquent

$$\hat{A}'_F \wedge \hat{A}'_1 \wedge \Lambda y_1 (\varphi_1 y_1 = y_1) \wedge \cdots \wedge \Lambda y_p (\varphi_p y_p = y_p) \wedge \wedge \text{Ext}_1(\mathscr{L}_1, \mathscr{L}'_1) \vdash (\neg \check{A}_F \vee \check{B}_1)$$

dans la notation du Chapitre 3. On note que les symboles fonctionnels de $\hat{A}_F$, $\hat{A}'_1$ qui n'appartiennent pas à $\mathscr{L}_1 \cup \mathscr{L}'_1$ n'admettent comme arguments ou valeurs que des types de $\mathscr{L}'$, et ceux de $\neg \check{A}_F \vee \check{B}_1$ n'admettent que des types de $\mathscr{L}$. Les φ_j $(j \leqslant p)$ admettent comme arguments des types de $\mathscr{L}$ et comme valeurs des types de $\mathscr{L}'$. Par conséquent tout terme de $\hat{\mathscr{L}}'_1 \cup \check{\mathscr{L}}_1$ dont la *valeur* a un type dans $\mathscr{L}$ est aussi un terme de $\check{\mathscr{L}}_1$. Il existe une formule V de $\check{\mathscr{L}}_1$ sans quantificateur (Ex. 3 du Chap. 5) telle que

(i) $\quad \hat{A}'_F \wedge \hat{A}'_1 \wedge \cdots \wedge \Lambda y_j (\varphi_j y_j = y_j) \wedge \cdots \wedge \text{Ext}_1(\mathscr{L}_1, \mathscr{L}'_1) \vdash V$

et

(ii) $\quad V \to (\neg \check{A}_F \vee \check{B}_1)$

V ne contenant pas de symbole appartenant à $\hat{\mathscr{L}}$. Le (i) entraîne que

$$\mathscr{A}' \cup \{ A'_1 \wedge \cdots \wedge \Lambda y_j \mathsf{V} y'_j (y'_j = y_j) \wedge \cdots \wedge \text{Ext}_1(\mathscr{L}_1, \mathscr{L}'_1) \} \vdash V;$$

en identifiant les langages $\mathscr{L}$, $\mathscr{L}'$, on a aussi $\mathscr{A} \vdash A_1 \to V$. De même, $\mathscr{A} \vdash V \to B_1$. On complète la démonstration en éliminant les symboles de $\check{\mathscr{L}}_1 - \mathscr{L}_1$ dans V au moyen des quantificateurs universels de $\mathscr{L}$.

3. On utilise les notations du chapitre 5 (théorie des types). Si σ, $\sigma' \in [\tau]$ on écrit, par abus de langage, $\sigma \in \sigma'$ si $\sigma' = (\sigma_1, ..., \sigma_n)$ et s'il existe $i\,(1 \leqslant i \leqslant n)$ tel que $\sigma = \sigma_i$; et on écrit $y_i^{\sigma_i}\, \varepsilon x^{\sigma'}$ pour

$$\bigvee_{j \neq i} \dots y_j^{\sigma_j} \dots [(y_1^{\sigma_1}, ..., y_i^{\sigma_i}, ..., y_n^{\sigma_n})\, \varepsilon_{\sigma'}\, x^{\sigma'}] .$$

La formule $A = Q_1 x_1 \dots Q_m x_m A_1$ est appelée Σ-formule si A_1 (sans quantificateur) a la forme

$$(x_{i_1} \varepsilon t_1 \wedge \cdots \wedge x_{i_k} \varepsilon t_k) \to B ,$$

où $i_1 < i_2 < \cdots < i_k$ est la liste des indices des quantificateurs Qx universels et où $t_j\,(1 \leqslant j \leqslant k)$ désigne soit x_n pour un $n < i_j$, soit une constante de A_1, soit une variable libre de A. (Une Σ-formule est donc une formule existentielle si on laisse de côté chaque variable qui est restreinte comme ci-dessus.)

Soit $\mathscr{L}_1^\tau$ le langage homotype au langage $\mathscr{L}^\tau$ (voir p. 112).

a) Montrer que $\mathfrak{M}_1$ est une τ-extension de $\mathfrak{M}$ si et seulement si $\mathfrak{M} \oplus \mathfrak{M}_1$ est une τ-réalisation du langage $\mathscr{L} \cup \mathscr{L}_1$ satisfaisant l'ensemble des formules τ-Ext $(\mathscr{L}, \mathscr{L}_1)$ qui consiste en Ext $(\mathscr{L}^\tau, \mathscr{L}_1^\tau)$ augmenté des formules

$$\bigwedge x^\sigma \bigwedge x_1^\sigma \bigwedge y_1^\tau \bigvee y^\tau [(x^\sigma = x_1^\sigma \wedge y_1^\tau\, \varepsilon_1\, x_1^\sigma) \to y^\tau = y_1^\tau] \text{ pour tout } \sigma \in [\tau] .$$

b) Monter que toute Σ-formule est stable pour les σ-extensions.

c) Trouver une τ-réalisation $\mathfrak{M}$ et une extension $\mathfrak{N}$ de $\mathfrak{M}$ telle que $\mathfrak{N}$ soit une τ-réalisation sans être une τ-extension de $\mathfrak{M}$. En déduire une Σ-formule A qui n'est pas stable pour toutes les extensions de $\mathfrak{M}$.

Solution.

a) et *b*) sont évidents. (On note que la réciproque de *b*) est vraie aussi ; on la démontre en utilisant *a*) et la méthode de l'exercice 2.)

c) Soit $\tau = (0)$, et soit $\mathscr{L}$ le langage à un seul symbole relationnel P, P ayant une seule variable. On prend pour $\mathfrak{M}$:

$E_0 = \{ a \}$, $E_{(0)} = \{ \{ a \} \}$, $a \in \overline{P}$ (E_0, $E_{(0)}$ sont les ensembles de base de $\mathfrak{M}$) ; et pour $\mathfrak{N}$:

$$U_0 = \{ a, b \}\ a \neq b,\ U_{(0)} = E_{(0)}\ ;\ a \in \overline{P}\ ;\ a \bar{\varepsilon}_{(0)} \{ a \},\ b\, \bar{\varepsilon}_{(0)} \{ a \}$$

($\bar{\varepsilon}_{(0)}$ étant la réalisation de $\varepsilon_{(0)}$ dans $\mathfrak{N}$).

Si on prend pour A la formule

$$\bigvee x^{(0)} \bigwedge z (z \varepsilon x^{(0)} \to Pz)$$

A est une Σ-formule, et A est satisfaite dans $\mathfrak{M}$ mais non dans $\mathfrak{N}$.

4. On utilise les notations de l'exercice 3. Si σ, $\sigma' \in [\tau]$, la notation $y^\sigma\ \varepsilon[x^{\sigma'}]$ (qui se lit : y appartient à la clôture transitive de x) désigne la disjonction des formules

$$y^\sigma \varepsilon x^{\sigma'} \quad \text{et} \quad \vee x_{i_1} \dots \vee x_{i_{n_i}} (y^\sigma \varepsilon x_{i_1} \varepsilon x_{i_2} \dots \varepsilon x_{i_{n_i}} \varepsilon x^{\sigma'}) ,$$

où $(i_1, \dots, i_{n_i})$ parcourt l'ensemble de toutes les suites finies satisfaisant : $\sigma \in \tau_{i_1} \in \tau_{i_2} \dots \tau_{i_{n_i}} \in \sigma'$, x_{i_j} ayant le type τ_{i_j}.

Une formule A, dont les variables libres sont $x_1, \dots, x_n$ est dite $\mathscr{A}$-τ-invariante si, pour tout couple $\mathfrak{M}$, $\mathfrak{M}'$ de τ-modèles de $\mathscr{A}$ tels que les restrictions de $\mathfrak{M}$ et de $\mathfrak{M}'$ à $E_0 \cap E'_0$ soient égales, et pour tout n-uplet $(\bar{x}_1, \dots, \bar{x}_n)$ appartenant à la τ-intersection de $\mathfrak{M}$ et de $\mathfrak{M}'$, ou bien $(\bar{x}_1, \dots, \bar{x}_n)$ satisfait A dans les deux modèles, ou bien $(\bar{x}_1, \dots, \bar{x}_n)$ satisfait $\neg A$ dans ces modèles.

Une formule prénexe $Q_1 y_1 \dots Q_k y_k B_1$, B_1 sans quantificateur, est dite restreinte (à $[x_1^{\tau_1}], \dots, [x_n^{\tau_n}]$) si B_1 a la forme

$$(y_{i_1} \varepsilon[t_1] \wedge \dots \wedge y_{i_p} \varepsilon[t_p]) \rightarrow [(y_{j_1} \varepsilon[s_1]) \wedge \dots \wedge (y_{j_q} \varepsilon[s_q]) \wedge C] ,$$

où $Q_{i_1}, \dots, Q_{i_p}$ sont les quantificateurs universels de la liste $Q_1, \dots, Q_k$, et $Q_{j_1}, \dots, Q_{j_q}$ les quantificateurs existentiels, et où t_r $(1 \leqslant r \leqslant p)$, s_r $(1 \leqslant r \leqslant q)$ désignent soit des constantes d'individu soit des variables. Montrer que A est $\mathscr{A}$-τ-invariante si et seulement s'il existe une formule restreinte B telle que $\mathscr{A} \vdash (A \leftrightarrow B)$.

b) Soit $\mathscr{A}$ tel que si $\mathfrak{M}$ et $\mathfrak{M}'$ sont des τ-modèles de $\mathscr{A}$ et si $E_0 \cap E'_0 \neq \phi$, l'intersection de $\mathfrak{M}$ et de $\mathfrak{M}'$ est aussi un τ-modèle de $\mathscr{A}$. Montrer que si A et $\neg A$ sont toutes deux $\mathscr{A}$-stables pour les τ-extensions, A est $\mathscr{A}$-τ-invariante. En déduire que si C_1 et C_2 sont deux Σ-formules telles que $\mathscr{A} \vdash (C_1 \leftrightarrow \neg C_2)$, C_1 et C_2 sont $\mathscr{A}$-τ-invariantes.

Solution.

a) On considère trois langages : $\mathscr{L}_0^{\tau'}$ est la restriction de $\mathscr{L}^\tau$ aux types $\sigma \in [\tau']$ où $\tau' = (\tau_1, \dots, \tau_n)$ et on ajoute n constantes $a_1^{\tau_1}, \dots, a_n^{\tau_n}$; $\mathscr{L}_1^\tau$ est obtenu en remplaçant, dans $\mathscr{L}^\tau$, ε par un nouveau symbole ε_1 et chaque type de variable $x, y, \dots$ par $x_1, y_1, \dots$; $\mathscr{L}_2^\tau$ est obtenu de la même façon sauf que ε est remplacé par ε_2 et les variables par $x_2, y_2, \dots$

Si A est $\mathscr{A}$-τ-invariante

$$\mathscr{A}_1 \cup \mathscr{A}_2 \cup \tau'\text{-Ext}(\mathscr{L}_0, \mathscr{L}_1) \cup \tau'\text{-Ext}(\mathscr{L}_0, \mathscr{L}_2) \cup$$
$$\cup\ TC(a_1^{\tau_1}, \dots, a_n^{\tau_n}) \vdash A_1(a_1, \dots, a_n) \leftrightarrow A_2(a_1, \dots, a_n)$$

où $TC(a_1^{\tau_1} \dots, a_n^{\tau_n})$ exprime, dans le langage $\mathscr{L}_0^\tau$, que tout objet appartient

à la clôture transitive de la réunion $a_1^{\tau_1} \cup \cdots \cup a_n^{\tau_n}$: c'est-à-dire pour tout σ tel que $\sigma \in [\tau_1] \vee \cdots \vee \sigma \in [\tau_n]$,

$$\wedge y^\sigma (y^\sigma \, \varepsilon [a_1^{\tau_1}] \vee \cdots \vee y^\sigma \, \varepsilon [a_n^{\tau_n}]) .$$

En séparant les différents types des variables et en appliquant le lemme d'interpolation avec égalité on trouve une formule B' du langage $\mathscr{L}_0$ telle que

$$\mathscr{A}_1 \cup \tau' - \text{Ext}\,(\mathscr{L}_0, \mathscr{L}_1) \cup TC \vdash A_1 \to B$$

et

$$\mathscr{A}_2 \cup \tau' - \text{Ext}\,(\mathscr{L}_0, \mathscr{L}_2) \cup TC \vdash B' \to A_2 .$$

Les ensembles de formules τ'-Ext $(\mathscr{L}_0, \mathscr{L}_1)$ et TC sont satisfaits en remplaçant ε de $\mathscr{L}_0^\tau$ par ε_1, et toute variable x de $\mathscr{L}_0^{\tau'}$ par

$$x_1 \, \varepsilon_1 [a_1^{\tau_1}] \vee \cdots \vee x_1 \, \varepsilon_1 [a_n^{\tau_n}] .$$

Par conséquent, B' prend la forme B cherchée.

Il est évident que toute formule B de cette forme est τ-invariante.

b) Soit $\mathfrak{M}_0$ la τ-intersection de $\mathfrak{M}$ et de $\mathfrak{M}'$ et soit $\bar{x}_i (1 \leqslant i \leqslant n)$ un élément de l'ensemble de base du type τ_i de $\mathfrak{M}_0$. $\mathfrak{M}$ étant une τ-extension de $\mathfrak{M}_0$, ou bien $(\bar{x}_1, \ldots, \bar{x}_n)$ satisfait A dans $\mathfrak{M}$ et dans $\mathfrak{M}_0$, ou bien $(\bar{x}_1, \ldots, \bar{x}_n)$ satisfait $\neg A$ dans $\mathfrak{M}$ et dans $\mathfrak{M}_0$. De même pour $\mathfrak{M}'$. Par conséquent, A est $\mathscr{A}$-τ-invariante. Puisque, d'après l'exercice 3(*b*), toute Σ-formule est stable pour les τ-extensions, C_1 et C_2 sont toutes deux τ-stables ; puisque $\mathscr{A} \vdash (\neg C_1) \leftrightarrow C_2$, C_1 et $\neg C_1$ sont $\mathscr{A}$-stables pour les τ-extensions et par conséquent $\mathscr{A}$-τ-invariantes.

5. On modifie les notations des exercices 3 et 4 comme suit : on dit que $\mathfrak{M}'$ est une $(\tau\,; 0)$-extension de $\mathfrak{M}$ lorsque $\mathfrak{M}$ et $\mathfrak{M}'$ sont des τ-réalisations, $\mathfrak{M}'$ est une τ-extension de $\mathfrak{M}$ et que $E_0 = E_0'$ (Ex. 3). Une formule A est dite $\mathscr{A}$-$(\tau\,; 0)$-invariante si, pour tout couple $\mathfrak{M}$, $\mathfrak{M}'$ de τ-modèles de $\mathscr{A}$ telles que $E_0 = E_0'$ et que les restrictions de $\mathfrak{M}$ et $\mathfrak{M}'$ à E_0 soient égales, et pour tout n-uplet $(\bar{x}_1, \ldots, \bar{x}_n)$ appartenant à leur τ-intersection, on a

$$(\bar{x}_1, \ldots, \bar{x}_n) \in \bar{A} \Leftrightarrow (\bar{x}_1, \ldots, \bar{x}_n) \in \bar{A}' .$$

On obtient les notions de Σ-$(\tau\,; 0)$-formule, resp. de formule $(\tau\,; 0)$-restreinte en supprimant toute restriction pour les variables de type 0 dans la définition de Σ-formule, resp. de formule restreinte.

a) Montrer que A est $\mathscr{A}$-$(\tau\,; 0)$-invariante si et seulement si il existe une formule B qui est $(\tau\,; 0)$-restreinte aux variables libres de A et telle que $\mathscr{A} \vdash (A \leftrightarrow B)$.

b) Soit $\mathscr{A}$ un ensemble de formules closes de $\mathscr{L}^\tau$ tel que pour tout τ-modèle de $\mathscr{A}$, son extension principale (Chap. 5) soit aussi un τ-modèle de $\mathscr{A}$. Montrer que si A et $\neg A$ sont toutes les deux $\mathscr{A}$-stables pour les $(\tau\,;0)$-extensions, elles sont aussi $\mathscr{A}$-$(\tau\,;0)$-invariantes.

c) Trouver un contre-exemple à l'énoncé obtenu à partir de (*b*) en remplaçant « $(\tau\,;0)$ » par « τ ».

Solution.

a) Soient $x_1^{\tau_1}, \ldots, x_n^{\tau_n}$ les variables libres de A de type $\neq 0$. On ajoute les constantes $a_1^{\tau_1}, \ldots, a_n^{\tau_n}$ (voir Ex. 4(*a*)) et on écrit $TC_0(a_1^{\tau_1}, \ldots, a_n^{\tau_n})$ pour la conjonction pour tout $\sigma \neq 0$ des formules $\wedge y^\sigma(y^\sigma\, \varepsilon[a_1^{\tau_1}] \vee \cdots \vee y^\sigma\, \varepsilon[a_n^{\tau_n}])$. On introduit les langages $\mathscr{L}_0^\tau, \mathscr{L}_1^\tau, \mathscr{L}_2^\tau$ et le type τ' comme dans l'exercice 4(*a*). Si A est $(\tau'\,;0)$-invariante on a :

$$\begin{aligned}\mathscr{A}_1 \cup \mathscr{A}_2 \cup \tau'\text{-Ext}\,(\mathscr{L}_0, \mathscr{L}_1) \cup \tau'\text{-Ext}\,(\mathscr{L}_0, \mathscr{L}_2) \cup \\ \cup \{\wedge x_1^0 \vee x_2^0(x_1^0 = x_2^0), \wedge x_2^0 \vee x_1^0(x_1^0 = x_2^0)\} \cup \\ \cup\, TC_0(a_1^{\tau_1}, \ldots, a_n^{\tau_n}) \vdash A_1(a_1^{\tau_1}, \ldots, a_n^{\tau_n}) \leftrightarrow A_2(a_1^{\tau_1}, \ldots, a_n^{\tau_n})\,.\end{aligned}$$

On trouve, par le lemme d'interpolation, une formule B' de $\mathscr{L}_0$ telle que

$$\mathscr{A}_1 \cup \tau'\text{-Ext}\,(\mathscr{L}_0, \mathscr{L}_1) \cup \{\wedge x_1^0 \vee x_0^0(x_0^0 = x_1^0)\} \cup TC_0(a_1^\tau, \ldots, a_n^\tau) \vdash A_1 \leftrightarrow B'$$

si l'on remplace ε par ε_1 et toute variable x de $\mathscr{L}_0$ de type $\neq 0$ par

$$x_1\, \varepsilon_1[a_1^{\tau_1}] \vee \cdots \vee x_1\, \varepsilon_1[a_n^{\tau_n}]\,,$$

B' prend la forme cherchée. La réciproque est évidente.

b) Soient $\mathfrak{M}$ et $\mathfrak{M}'$ deux τ-modèles de $\mathscr{A}$ tels que $E_0 = E_0'$ et que les restrictions de $\mathfrak{M}$ et de $\mathfrak{M}'$ à E_0 soient égales. Par conséquent, les extensions principales de $\mathfrak{M}$ et de $\mathfrak{M}'$ sont aussi égales. Si $\mathfrak{M}_0$ désigne l'extension principale commune et si $\bar{x}_i$ appartient à la τ-intersection de $\mathfrak{M}$ et de $\mathfrak{M}'$, $\bar{x}_i$ appartient aussi à l'ensemble de base de type τ_i de $\mathfrak{M}_0$ $(1 \leqslant i \leqslant n)$. Puisque $\mathfrak{M}_0$ est une $(\tau\,;0)$-extension de $\mathfrak{M}$, et que A et $\neg A$ sont $\mathscr{A}$-$(\tau\,;0)$-stables,

$$(\bar{x}_1^{\tau_1}, \ldots, \bar{x}_n^{\tau_n}) \in \bar{A} \leftrightarrow (\bar{x}_1^{\tau_1}, \ldots, \bar{x}_n^{\tau_n}) \in \bar{A}_0\,.$$

De même pour le couple $\mathfrak{M}'$, $\mathfrak{M}_0$. Par conséquent, A est $\mathscr{A}$-$(\tau\,;0)$-invariante.

c) Soit $\mathscr{A}_1$ un ensemble de formules du langage $\mathscr{L}$ du premier ordre tel qu'il existe deux formules existentielles A_1, A_2 à une seule variable x satisfaisant $\mathscr{A}_1 \vdash (A_1 \leftrightarrow \neg A_2)$ sans qu'il existe une formule A' sans

quantificateur telle que $\mathscr{A} \vdash (A_1 \leftrightarrow A')$ (Ex. 1, *e*)). On considère $\mathscr{L}^{(0)}$, et on pose

$$\mathscr{A} = \mathscr{A}_1 \cup \bigwedge x^{(0)} \bigwedge y^{(0)}[\bigwedge z^0(z\varepsilon x \leftrightarrow z\varepsilon y) \rightarrow x = y] .$$

Evidemment $\mathscr{A}$ satisfait les hypothèses de (*b*). On prend

$$A = \bigwedge x^0(x\varepsilon X \rightarrow A_1) ,$$

où X est une variable de type (0). Puisque

$$\mathscr{A} \vdash \neg A \leftrightarrow \bigvee x(x\varepsilon X \wedge A_2) ,$$

A et $\neg A$ sont $\mathscr{A}$-stables pour les τ-extensions. Mais A n'est pas $\mathscr{A}$-τ-invariante car il n'existe aucune formule B restreinte à $[X]$ telle que $\mathscr{A} \vdash A \leftrightarrow B$. En effet, si dans une telle B on prend $\bar{X} = \{ u \}$, ce qui revient à remplacer toute partie de la forme $y\varepsilon X$ dans B par $y = u$, on obtiendrait une formule sans quantificateur.

6. *a*) Montrer que (i) le corps des rationnels réels est rigidement contenu dans tout corps commutatif de caractéristique 0, (ii) le corps des rationnels complexes est contenu, mais non ridigement contenu, dans tout corps commutatif algébriquement fermé de caractéristique 0.

b) Soit $\mathscr{L}$ le langage (ensembliste) dont le seul symbole relationnel est ε ; soit A la conjonction des formules

$$\bigvee x \bigwedge y \neg y\varepsilon x, \bigwedge x \bigwedge y \bigvee z \bigwedge u[u\varepsilon z \leftrightarrow (u\varepsilon x \vee u = y)] ,$$
$$\bigwedge x \bigwedge y[\bigwedge z(z\varepsilon x \leftrightarrow z\varepsilon y) \rightarrow x = y]$$

et soit $\mathscr{L}_1$ le langage obtenu en ajoutant à $\mathscr{L}$ la constante d'individu c et le symbole relationnel à 3 variables R. On pose

$$B = \bigwedge y \neg y\varepsilon c \wedge \bigwedge x \bigwedge y \bigwedge z(R(x, y, z) \leftrightarrow \bigwedge u[u\varepsilon z \leftrightarrow (u\varepsilon x \vee u = y)]) .$$

Montrer que (i) aucune réalisation de $\mathscr{L}$ n'est rigidement contenue dans tous les modèles de A, (ii) tout modèle de A s'étend d'une seule façon en un modèle de B, (iii) la réalisation de $\mathscr{L}_1$ dont l'ensemble d'individus est l'ensemble C_ω des ensembles héréditairement finis, où $\bar{\varepsilon}$ est $\in \cap (C_\omega \times C_\omega)$, où $\bar{c}$ est l'ensemble vide, et où $\bar{R}$ est la relation $z = x \cup \{ y \}$, est rigidement contenue dans tous les modèles de $A \wedge B$.

Solution.

a) Le (i) est évident même si l'on supprime les constantes 0 et 1 du langage des corps ; utilisant les notations du théorème 3 on prend pour $A_0(x, x_1)$ la formule $x_1 + x = x_1$, et pour $A_1(x, x_1)$ la formule $(x.x_1 = x_1 \wedge x \neq x_1)$. (ii) L'application $z \rightarrow \bar{z}$ (où $\bar{z}$ désigne le conjugué

de z) montre que le corps des rationnels complexes n'est même pas rigidement contenu dans lui-même.

b) (i) Une réalisation de $\mathscr{L}$ (d'ailleurs contenue dans tous les modèles de A) est $\langle C_\omega, \in \cap (C_\omega \times C_\omega) \rangle$. Or elle n'est pas rigidement contenue dans elle-même parce qu'elle est isomorphe a toute sous-réalisation C_ω^a ainsi définie : C_ω^a est la plus petite classe contenant a qui est close par rapport à l'opération $x, y \to x \cup \{ y \}$. (ii) A implique l'existence d'un ensemble vide et (grâce au troisième axiome, axiome d'extensionnalité) d'un seul ; par conséquent, la valeur de c est déterminée. Ainsi l'extensionnalité détermine la valeur de R, étant donné un modèle de A. (iii) est évident parce que tout élément de C_ω peut être engendré à partir de l'ensemble vide par l'opération $x \cup \{ y \}$.

7. On considère un langage $\mathscr{L}$ à un seul type et le langage $\mathscr{L}^\tau$ qui lui est associé dans le chapitre 5. On suppose que $\mathscr{L}$ contient un ensemble **C** de constantes d'individu. Soit $\mathscr{A}$ un ensemble de formules de $\mathscr{L}$ qui possède un **C**-modèle : pour tout couple (c, c'), c et c' éléments distincts de **C**, $\mathscr{A} \vdash \neg c = c'$. Pour $\sigma \in [\tau]$, un ensemble X^σ de l'échelle des types construite sur **C** est dit *appartenir* à une réalisation $\mathfrak{N}^\tau$ de $\mathscr{A}^\tau$ si X^σ est l'image d'un élément de $\mathfrak{N}^\tau$ de type σ par l'application canonique de $\mathfrak{N}^\tau$ dans $\mathfrak{N}_0^\tau$, où $\mathfrak{N}_0$ est un **C**-modèle isomorphe à la restriction de $\mathfrak{N}^\tau$ au type 0, et où $\mathfrak{N}_0^\tau$ est la réalisation principale sur $\mathfrak{N}_0$. Montrer que, si X^σ appartient à toute **C**-réalisation de $\mathscr{A}$, alors X est héréditairement fini sur **C**.

Solution.

L'ensemble X^0 des éléments de type 0 qui appartiennent à la clôture transitive de X^σ est défini, dans tout modèle, par la disjonction des formules

$$\vee x_1^{\tau_1} \dots \vee x_r^{\tau_r} (x \varepsilon x_1^{\tau_1} \varepsilon x_2^{\tau_2} \dots \varepsilon x_r^{\tau_r} \varepsilon a^\sigma)$$

où $(\tau_1, \dots, \tau_n)$ parcourt toutes les suites finies telles que $0 \in \tau_1 \in \cdots \in \tau_\tau \in \sigma$ (en utilisant les notations de l'Exercice 3). La constante a^σ désigne l'ensemble X^σ qui, par hypothèse, appartient à tout modèle de $\mathscr{A}$. D'après le Théorème 4, X^0 est donc fini, et par conséquent X^σ est héréditairement fini.

8. Si $\mathscr{A}$ est un ensemble dénombrable de formules closes du langage $\mathscr{L}$ possédant un **C**-modèle et si X ($X \subset$ **C**) est définissable *sur* **C** dans tous les **C**-modèles de $\mathscr{A}$ il existe une formule close B et une formule Ax à une seule variable libre x telles que $\mathscr{A} \vdash B \to Ac$ si $c \in X$ et $\mathscr{A} \vdash B \to \neg Ac$ si $c \notin X$.

Solution.

D'après le théorème 5 il existe une famille *finie* de formules $F_j(x_1, ..., x_n)$ $(j < N)$ et $A_1(x, x_1, ..., x_n)$ telles que

$$\mathscr{A} \cup \{ \bigvee x_1 ... \bigvee x_n(F_1 \wedge \cdots \wedge F_{N-1}) \}$$

ait un modèle et

$$\mathscr{A} \vdash \bigwedge x_1 ... \bigwedge x_n[(F_1 \wedge \cdots \wedge F_{N-1}) \rightarrow A_1(c, x_1, ..., x_n)] \quad \text{si} \quad c \in X ,$$

$$\mathscr{A} \vdash \bigwedge x_1 ... \bigwedge x_n[(F_1 \wedge \cdots \wedge F_{N-1}) \rightarrow \neg A_1(c, x_1, ..., x_n)] \quad \text{si} \quad c \notin X .$$

On prend pour B :

$$\bigvee x_1 ... \bigvee x_n(F_1 \wedge \cdots \wedge F_{N-1})$$

et pour Ax :

$$\bigvee x_1 ... \bigvee x_n(F_1 \wedge \cdots \wedge F_{N-1} \wedge A_1) .$$

Si $c \in X$, $\mathscr{A} \vdash B \rightarrow Ac$; si $c \notin X$, $\mathscr{A} \vdash \neg Ac$ et, à plus forte raison, $\mathscr{A} \vdash (B \rightarrow \neg Ac)$.

9. Soit $\mathscr{L}_0$ le langage des corps ordonnés et soit $\mathscr{A}_0$ l'ensemble des axiomes pour les corps réels fermés (Ch. 4). On considère un ensemble $\mathbf{C}$ de constantes pour représenter chaque rationnel, et des langages $\mathscr{L}$ obtenus en ajoutant des constantes d'individu supplémentaires à $\mathscr{L}_0$. Donner des contre-exemples aux énoncés suivants :

a) Si $\mathscr{A}$ est dénombrable et si $X(X \subset \mathbf{C})$ est définissable sur $\mathbf{C}$ dans tous les $\mathbf{C}$-modèles de $\mathscr{A}$, il existe une formule Ax de $\mathscr{L}$ telle que, pour tout $c \in \mathbf{C}$, $\mathscr{A} \vdash Ac$ si $c \in X$, et $\mathscr{A} \vdash \neg Ac$ si $c \notin X$.

b) Si X est définissable dans tous les $\mathbf{C}$-modèles de $\mathscr{A}$, il existe une formule close B et une formule Ax telles que $\mathscr{A} \cup \{ B \}$ a un modèle et, pour tout $c \in \mathbf{C}$, $\mathscr{A} \vdash (B \rightarrow Ac)$ si $c \in X$, $\mathscr{A} \vdash (B \rightarrow \neg Ac)$ si $c \notin X$. (On ne suppose évidemment pas que $\mathscr{A}$ est dénombrable.)

Solution.

On prend pour X une coupure des rationnels qui n'est pas définissable dans le langage $\mathscr{L}_0$. Un tel X existe parce que l'ensemble des coupures est non dénombrable tandis que l'ensemble des coupures définissables $X = \{ c : \mathscr{A}_0 \vdash Ac \}$ $(Ax \in \mathscr{L}_0)$ est dénombrable. On cherche deux ensembles d'axiomes $\mathscr{A} \supset \mathscr{A}_0$ tels que X soit définissable sur $\mathbf{C}$ dans tout modèle de $\mathscr{A}$.

a) On ajoute à $\mathscr{L}_0$ deux constantes d'individu u et v et on prend

$$\mathscr{A}_1 = \{(c < u < c') \vee (c < v < c') : \text{pour tout couple } (c, c'),\ c \in X,\ c' \in -X \} ,$$

et on pose $\mathscr{A} = \mathscr{A}_0 \cup \mathscr{A}_1$. X est défini, dans tout modèle de $\mathscr{A}$, ou bien par la formule $x < u$, ou bien par la formule $x < v$. Supposons que Ax est une formule de $\mathscr{L}$ telle que $\mathscr{A} \vdash Ac$ si $c \in X$, $\mathscr{A} \vdash \neg Ac$ si $c \notin X$; puisque Ax est une formule de $\mathscr{L}$, il existe une formule $Bxyz$ de $\mathscr{L}_0$ telle que $Ax = Bxuv$. Considérons les modèles $\mathfrak{M}$ dont l'ensemble de base est $\mathbf{R}$ (nombres réels) avec l'ordre usuel et qui satisfont $\mathscr{A}$ (c'est-à-dire, ou bien $\bar{u}$ = la coupure X, ou bien $\bar{v} = X$). Si $\bar{u} = X$, $\bigvee y \bigwedge z\, B(c, y, z)$ est vraie dans $\mathfrak{M}$ pour $c \in X$; si $\bar{v} = X$, $\neg \bigvee y \bigwedge z B(c, y, z)$ est vraie dans $\mathfrak{M}$ pour $c \notin X$. Puisque $\bigvee y \bigwedge z B(x, y, z)$ est une formule de $\mathscr{L}_0$ et que $\mathscr{A}_0$ est saturé, pour tout $c \in \mathbf{C}$, on a : $\mathscr{A}_0 \vdash \bigvee y \bigwedge z B(c, y, z)$ si $c \in X$ et $\mathscr{A}_0 \vdash \neg \bigvee y \bigwedge z B(c, y, z)$ si $c \notin X$. Ce qui contredit la condition que X n'est pas définissable dans $\mathscr{L}_0$.

b) On ajoute à $\mathscr{L}_0$ les constantes d'individu u_α ($\alpha < \aleph_1$), on considère une énumération $c_1, c_2, \ldots$, des éléments de X et on pose

$$\mathscr{A}_1 = \{ u_\alpha < c : c \in \mathbf{C} - X, \alpha < \aleph_1 \} \cup$$
$$\cup \{ u_\alpha \neq u_\beta : \alpha \neq \beta, \alpha, \beta < \aleph_1 \}$$
$$\cup \{ (u_{\alpha_0} < u_{\alpha_1} < \cdots < u_{\alpha_j}) \to c_j < u_{\alpha_j} : \alpha_i < \aleph_1, i \leqslant j,$$

pour tout entier $j \}$.

$\mathscr{A}_0 \cup \mathscr{A}_1$ a un modèle $\mathfrak{M}$, parce que tout sous-ensemble fini a évidemment un modèle. De plus X est définissable dans tout modèle de $\mathscr{A}_0 \cup \mathscr{A}_1$ parce qu'un ordre total non dénombrable possède au moins un élément avec un nombre infini de prédécesseurs. Si u_α est un tel élément, $x < u_\alpha$ définit X sur $\mathbf{C}$ dans le modèle considéré.

Pour établir *b*), supposons que B_1, B_2x sont deux formules de $\mathscr{L}$; il existe donc deux formules $C_1(x_0, \ldots, x_p)$, $C_2(x_0, \ldots, x_p, x)$ de $\mathscr{L}_0$ telles que

$$B_1 = C_1(u_{\alpha_0}, \ldots, u_{\alpha_p}) \qquad \text{et} \qquad B_2x = C_2(u_{\alpha_0}, \ldots, u_{\alpha_p}, x)\,.$$

Si, pour $c \in \mathbf{C}$,

$$\mathscr{A} \cup \mathscr{A}_1 \vdash (B_1 \to B_2c) \qquad \text{pour} \qquad c \in X\,,$$

et

$$\mathscr{A}_0 \cup \mathscr{A}_1 \vdash (B_1 \to \neg B_2c) \qquad \text{pour} \qquad c \notin X\,,$$

$\mathbf{C}$ étant dénombrable, il existe un sous-ensemble dénombrable $\mathscr{A}_1'$ de $\mathscr{A}_1$ tel que

$$\mathscr{A} \cup \mathscr{A}_1' \vdash (B_1 \to B_2c) \qquad \text{pour} \qquad c \in X\,,$$
$$\mathscr{A}_0 \cup \mathscr{A}_1' \vdash (B_1 \to \neg B_2c) \qquad \text{pour} \qquad c \notin X\,.$$

Soit u_{α_n} $(n = p + 1, p + 2, ...)$ une énumération des constantes u_α qui apparaissent dans $\mathscr{A}'_1$ (et non dans $B_1 \to B_2 c$), et supposons que

$$\bar{u}_{\alpha_0} < \cdots < \bar{u}_{\alpha_p} \text{ dans } \mathfrak{M} .$$

On pose

$$B^*(x_0, ..., x_p, y) = C_1(x_0, ..., x_p) \wedge c_0 < x_0 \wedge c_1 < x_1 \wedge \cdots$$
$$\wedge\ c_p < x_p \wedge x_0 < x_1 < \cdots < x_p < y .$$

Puisque B_1 est vraie dans $\mathfrak{M}$ et que $\bar{u}_{\alpha_0} < \cdots < \bar{u}_{\alpha_p}$, la formule

$$\bigvee x_0 \ldots \bigvee x_p\, B^*(x_0, ..., x_p, c)$$

de $\mathscr{L}_0$ est vraie dans $\mathfrak{M}$ pour tout $c \in \mathbf{C} - X$ et puisque X n'est pas définissable dans $\mathscr{L}_0$, il existe c_k tel que $\bigvee x_0 \ldots \bigvee x_p\, B^*(x_0, ..., x_p, c_k)$ est vraie.

On va en déduire (i) et (ii) :

(i) Pour tout entier i,
$\bigwedge x_0 \ldots \bigwedge x_p[B^*(x_0, ..., x_p, c_k) \to C_2(x_0, ..., x_p, c_i)]$ est vraie dans $\mathfrak{M}$. Puisque par hypothèse

$$\mathscr{A} \cup \mathscr{A}'_1 \vdash C_1(u_{\alpha_0}, ..., u_{\alpha_p}) \to C_2(u_{\alpha_0}, ..., u_{\alpha_p}, c_i)$$

il suffit de noter que, si $B^*(\bar{x}_0, ..., \bar{x}_p, c)$ est vraie dans $\mathfrak{M}$, $\mathscr{A}_0 \cup \mathscr{A}'_1$ est satisfait dans le modèle $\mathfrak{M}'$ obtenu à partir de $\mathfrak{M}$ comme suit : on pose $\bar{u}_{\alpha_i} = \bar{x}_i$ $(i \leqslant p)$, et on prend pour $\bar{u}_{\alpha_n}$, $\bar{u}_{\alpha_{n+1}}$, ... une suite croissante d'éléments de l'ensemble de base de $\mathfrak{M}$ telle que $X > \bar{u}_{\alpha_m} > c_n$ pour tout $m > n$. Par conséquent, $C_2(u_{\alpha_0}, ..., u_{\alpha_p}, c_i)$ est vraie dans $\mathfrak{M}'$, et $C_2(x_0, ..., x_p, c_i)$ est donc vraie dans $\mathfrak{M}$. De même

(ii) Pour tout $c \in \mathbf{C} - X$,

$$\bigwedge x_0 \ldots \bigwedge x_p[B^*(x_0, ..., x_p, c_k) \to \neg\, C_2(x_0, ..., x_p, c)]$$

est vraie dans $\mathfrak{M}$.

Les (i), (ii) montrent que la formule de $\mathscr{L}_0$:

$$\bigwedge x_0 \ldots \bigwedge x_p[B^*(x_0, ..., x_p, c_k) \to \neg\, C_2(x_0, ..., x_p, x)]$$

définit X sur $\mathbf{C}$ dans $\mathfrak{M}$; puisque $\mathscr{A}_0$ est saturé pour $\mathscr{L}_0$, cette formule définit X dans tout modèle de $\mathscr{A}_0$, ce qui contredit le choix de X.

---

7. MODÈLES PRINCIPAUX ; MODÈLES DE FORMULES INFINIES

Résumé

La première partie de ce chapitre traite une classe importante de réalisations du langage des types finis décrit dans le chapitre 5 : celle des modèles principaux (ou « pleins ») où l'ensemble de base C_0 est quelconque, mais où le domaine de chacune des autres variables est constitué par *tous* les ensembles (du type correspondant) de la structure des types ayant pour base C_0. Le résultat essentiel réduit la validité dans les réalisations principales des langages d'ordre *fini* à la validité dans les réalisations principales de certains langages (convenablement choisis) du *second* ordre. Ainsi qu'il était annoncé dans le résumé du chapitre 3, cette dernière validité ne peut pas, en général, être réduite au cas du premier ordre, d'après l'exercice 5 du chapitre 3 et les exercices 1, 5. On donne une certaine classe de formules du second ordre qui équivalent à des ensembles infinis de formules du premier ordre : c'est la généralisation du théorème de plongement qui était aussi annoncée dans le résumé du chapitre 3.

Les systèmes infinis d'axiomes qu'on vient de mentionner (et ceux du chapitre précédent) peuvent être considérés comme des conjonctions infinies de formules finies. La seconde partie du présent chapitre étudie des langages contenant d'autres expressions *infiniment longues*, en particulier des formules $\Lambda x \bigvee\!\!\!\bigvee A_i x \ (i \in I)$, où $\bigvee\!\!\!\bigvee A_i$ désigne la disjonction infinie des formules finies $A_i \ (i \in I)$. L'exercice 5 donne une liste de structures courantes définies par de telles formules. Le résultat fondamental consiste en une caractérisation simple de la classe des formules finies qui sont valides dans tout modèle d'un système dénombrable d'axiomes A^m $(m = 1, 2, \ldots)$ de la forme $\Lambda x \bigvee\!\!\!\bigvee_n B_n^m x \ (n = 1, 2, \ldots)$. Ce résultat ne s'étend pas directement au cas non dénombrable (exercice 3). Pour des informations récentes sur le sujet (florissant) des formules infinies, voir le livre [*The Theory of Models*, Amsterdam (1965)], en particulier les articles de Karp, Keisler et Scott.

Les deux derniers résultats du chapitre précédent sont généralisés aux langages dont nous nous occupons ici ; ils revêtent une forme spécialement simple dans le cas des modèles de la théorie des types qui satisfont la formule infinie $\Lambda x \bigvee\!\!\!\bigvee (x = c_n)$, c'est-à-dire des modèles dont l'ensemble de base C_0 est égal à $\{ c_0, c_1, \ldots \}$.

Pour formuler des résultats plus fins sur les langages contenant de formules infinies et sur leurs réalisations, on a besoin des notions de la

théorie des fonctions récursives sur les ordinaux (infinis) ; même la généralisation du théorème de finitude au cas ci-dessus de la formule $\bigwedge x \bigvee_n (x = c_n)$ réclame les notions de la théorie de l'hyperarithméticité (récursivité sur les ordinaux récursifs). Cette théorie fournit aussi une explication du rôle particulier joué par la négation et la disjonction infinie parmi tous les connecteurs propositionnels à un nombre infini de variables. Voir les articles cités dans le résumé du chapitre précédent.

On considère les langages $\mathscr{L}^\tau$ de la théorie des types (Chap. 5). D'après le dernier théorème de ce chapitre on peut associer à toute réalisation $\mathfrak{M}$ de $\mathscr{L}$ une réalisation $\mathfrak{M}^\tau$ d'ordre τ de $\mathscr{L}$, qu'on appelle *réalisation principale d'ordre τ construite sur $\mathfrak{M}$*. Elle est unique à un isomorphisme près. Dans une réalisation principale la relation $\bar{\varepsilon}_\sigma(\sigma = (\sigma_1, ..., \sigma_n))$ sur $E_{\sigma_1} \times \cdots \times E_{\sigma_n} \times E_\sigma$ est isomorphe à la relation d'appartenance sur $E_{\sigma_1} \times \cdots \times E_{\sigma_n} \times \mathfrak{P}(E_{\sigma_1} \times \cdots \times E_{\sigma_n})$: pour *tout* sous-ensemble X de $E_{\sigma_1} \times \cdots \times E_{\sigma_n}$, il existe un élément a et un seul de E_σ dont les « éléments » dans la réalisation sont les éléments de X.

On appelle théorème d'ordre τ de $\mathscr{L}$, une formule d'ordre τ dont la clôture est satisfaite par toutes les réalisations principales d'ordre τ de $\mathscr{L}$.

Nous supposerons que $\mathscr{L}$ n'a pas de symboles fonctionnels, ce qui ne restreint pas la généralité : une formule F est en effet un théorème d'ordre τ si et seulement si la formule F^* qui lui est associée, Chap. 5, Ex. 1 (2), en est un.

Soit $\mathscr{L}_0$ le langage à un seul type de variable obtenu à partir de $\mathscr{L}^\tau$ en considérant toutes les variables comme de même type (et en conservant les symboles relationnels de $\mathscr{L}^\tau$, chacun gardant le même nombre de variables). Soit $\mathscr{L}^*$ le langage obtenu en ajoutant à $\mathscr{L}_0$ de nouveaux symboles relationnels à une variable : T_σ pour chaque $\sigma \leqslant \tau$. A chaque formule F de $\mathscr{L}^\tau$ on associe une formule F^* de $\mathscr{L}^*$, définie par récurrence sur la longueur de F de la façon suivante :

si $F(x_1^{\sigma_1}, ..., x_n^{\sigma_n})$ est atomique, $F^* = F(x_1, ..., x_n) \wedge T_{\sigma_1} x_1 \wedge \cdots \wedge T_{\sigma_n} x_n$

si $F(x_1^{\sigma_1}, ..., x_n^{\sigma_n}) = \neg G(x_1^{\sigma_1}, ..., x_n^{\sigma_n})$, alors

$$F^* = \neg G^*(x_1, ..., x_n) \wedge T_{\sigma_1} x_1 \wedge \cdots \wedge T_{\sigma_n} x_n$$

si $F = A(x_1^{\sigma_1}, ..., x_n^{\sigma_n}) \vee B(x_1^{\sigma_1}, ..., x_n^{\sigma_n})$ alors

$$F^* = (A^* \vee B^*) \wedge T_{\sigma_1} x_1 \wedge \cdots \wedge T_{\sigma_n} x_n$$

si $F = \bigvee x^\sigma G(x^\sigma, x_1^{\sigma_1}, ..., x_n^{\sigma_n})$, alors $F^* = \bigvee x[T_\sigma x \wedge G^*(x, x_1, ..., x_n)]$.

Les formules d'ordre (0) de $\mathscr{L}^*$ seront construites avec un nouvel ensemble de variables d'ordre (0) dont nous désignerons les éléments par X, Y, Z, ..., et un nouveau symbole relationnel à deux variables que nous noterons e.

Soit $\mathscr{U}$ la conjonction des formules suivantes d'ordre (0) de $\mathscr{L}^*$:

1) $\Lambda x \neg [T_\sigma x \wedge T_{\sigma'} x]$ pour tout couple σ, σ' de types distincts et $\leqslant \tau$;

2) $\Lambda x_1 \ldots \Lambda x_n \Lambda x[\varepsilon_\sigma(x_1, \ldots, x_n, x) \to T_{\sigma_1} x_1 \wedge \cdots \wedge T_{\sigma_n} x_n \wedge T_\sigma x]$
pour tout $\sigma \leqslant \tau$, $\sigma = (\sigma_1, \ldots, \sigma_n)$;

3) $\Lambda x \Lambda y[(\Lambda x_1 \ldots \Lambda x_n[\varepsilon_\sigma(x_1, \ldots, x_n, x) \leftrightarrow \varepsilon_\sigma(x_1, \ldots, x_n, y)]) \to x = y]$
pour tout $\sigma \leqslant \tau$; $\sigma = (\sigma_1, \ldots, \sigma_n)$;

4) $\Lambda x_1 \ldots \Lambda x_n \mathrm{V} y \{ T_{\sigma_1} x_1 \wedge \cdots T_{\sigma_n} x_n \to [T_\sigma y \wedge \varepsilon_\sigma(x_1, \ldots, x_n, y) \wedge$
$\wedge \Lambda u_1 \ldots \Lambda u_n[\varepsilon_\sigma(u_1, \ldots, u_n, y) \to (u_1 = x_1 \wedge \cdots \wedge u_n = x_n)]] \}$
pour tout $\sigma \leqslant \tau$, $\sigma = (\sigma_1, \ldots, \sigma_n)$;

5) $\Lambda X \mathrm{V} y \{ T_\sigma y \wedge \Lambda x_1 \ldots \Lambda x_n[\varepsilon_\sigma(x_1, \ldots, x_n, y) \leftrightarrow \mathrm{V} z(z \varepsilon X \wedge$
$\wedge \Lambda u_1 \ldots \Lambda u_n(\varepsilon_\sigma(u_1 \ldots u_n, z) \to u_1 = x_1 \wedge \cdots \wedge u_n = x_n)]\}$
pour chaque $\sigma \leqslant \tau$.

Les seules formules d'ordre (0) de $\mathscr{L}^*$ parmi les formules ci-dessus sont donc les formules 5). Les autres sont d'ordre 0.

THÉORÈME 1. — *Pour qu'une formule close F de $\mathscr{L}$, d'ordre τ, soit un théorème d'ordre τ il faut et il suffit que $\mathscr{U} \to F^*$ soit un théorème d'ordre* (0) *de $\mathscr{L}^*$.*

Soit $\mathfrak{M}^*$ un modèle de (1, 2, 3) dont l'ensemble de base est E^*. On en déduit une réalisation $\mathfrak{M}^\tau$ d'ordre τ de $\mathscr{L}$, dont l'ensemble de base de type σ est $\overline{T}_\sigma$ (valeur de T_σ dans $\mathfrak{M}^*$), en donnant aux symboles relationnels de $\mathscr{L}^\tau$ la valeur qu'ils prennent dans $\mathfrak{M}^*$. D'après 1) les ensembles de base de $\mathfrak{M}^\tau$ sont bien disjoints, et d'après 2) et 3) les axiomes d'extensionnalité sont bien satisfaits.

Toute réalisation $\mathfrak{M}^\tau$ d'ordre τ de $\mathscr{L}$ est ainsi obtenue à partir d'un modèle $\mathfrak{M}^*$ de (1, 2, 3) : soient en effet E_σ ($\sigma \leqslant \tau$) les ensembles de base de $\mathfrak{M}^\tau$. On définit l'ensemble de base E^* de $\mathfrak{M}^*$ comme $\bigcup_{\sigma \leqslant \tau} E_\sigma$. On définit la valeur de T_σ dans $\mathfrak{M}^*$ par $\overline{T}_\sigma = E_\sigma$. Les autres symboles relationnels de $\mathscr{L}^*$ sont des symboles de $\mathscr{L}^\tau$: on leur donne dans $\mathfrak{M}^*$ la même valeur que dans $\mathfrak{M}^\tau$. On voit immédiatement que $\mathfrak{M}^*$ satisfait (1, 2, 3) puisque $\mathfrak{M}^\tau$ satisfait $\mathscr{X}_\tau$ (p. 92).

Soit F une formule de $\mathscr{L}^\tau$. Alors les valeurs de F et F^* dans deux réalisations associées $\mathfrak{M}^\tau$ et $\mathfrak{M}^*$ de $\mathscr{L}^\tau$ et $\mathscr{L}^*$ sont égales. On le montre immédiatement par récurrence sur la longueur de F d'après la définition de F^*.

Soit alors $\mathfrak{M}^*$ un modèle principal de $\mathscr{U}$ dont l'ensemble d'individus (ensemble de base du type 0) est E^*. Alors la réalisation $\mathfrak{M}^\tau$ d'ordre τ de $\mathscr{L}$ qui lui est associée est aussi principale : il suffit de montrer que la relation $\bar{\varepsilon}_\sigma$ sur $\overline{T}_{\sigma_1} \times \cdots \times \overline{T}_{\sigma_n} \times \overline{T}_\sigma$ (où $\sigma = (\sigma_1, \ldots, \sigma_n) \leqslant \tau$ et où $\bar{\varepsilon}_\sigma$, $\overline{T}_{\sigma_i}$ sont les valeurs de ε_σ et T_{σ_i} dans $\mathfrak{M}^*$) est isomorphe à la relation d'appartenance sur

$$\overline{T}_{\sigma_1} \times \cdots \times \overline{T}_{\sigma_n} \times \mathfrak{P}(\overline{T}_{\sigma_1} \times \cdots \times \overline{T}_{\sigma_n}),$$

donc que pour tout sous-ensemble K de $\overline{T}_{\sigma_1} \times \cdots \times \overline{T}_{\sigma_n}$ il existe $a \in \overline{T}_\sigma$

dont les « éléments » dans $\mathfrak{M}^\tau$ sont les éléments de K. Soit $(a_1, ..., a_n)$ un élément quelconque de K. D'après 4) il existe un élément $\varphi(a_1, ..., a_n)$ de $\overline{T}_\sigma$ qui a $(a_1, ..., a_n)$ pour seul « élément » dans $\mathfrak{M}^\tau$. Comme $\mathfrak{M}^*$ est principale, il existe un élément X de l'ensemble de base de type (0) de $\mathfrak{M}^*$ dont les « éléments » dans $\mathfrak{M}^*$ sont les $\varphi(a_1, ..., a_n)$ pour $(a_1, ..., a_n) \in K$. D'après 5) il existe donc $y \in \overline{T}_\sigma$ dont les « éléments » dans $\mathfrak{M}^\tau$ sont les $(a_1, ..., a_n)$ de K.

Toute réalisation principale $\mathfrak{M}^\tau$ de $\mathscr{L}$ est ainsi obtenue, à partir d'un modèle principal $\mathfrak{M}^*$ de $\mathscr{U}$: on définit $\mathfrak{M}^*$ à l'ordre 0 comme ci-dessus. On a vu que (1, 2, 3) sont alors satisfaits. 4) est aussi satisfait puisque, $\mathfrak{M}^\tau$ étant principale, si $\sigma = (\sigma_1, ..., \sigma_n) \leqslant \tau$, et si $a_1 \in E_{\sigma_1}, ..., a_n \in E_{\sigma_n}$, il existe $a \in E_\sigma$ dont le seul « élément » dans $\mathfrak{M}^\tau$ est $(a_1, ..., a_n)$. On prend pour $\mathfrak{M}^*$ la réalisation principale d'ordre (0) construite sur la réalisation ainsi obtenue, et il est immédiat que $\mathfrak{M}^*$ satisfait 5).

Soit alors F une formule close de $\mathscr{L}^\tau$. Si F n'est pas un théorème d'ordre τ, il existe une réalisation principale $\mathfrak{M}^\tau$ d'ordre τ de $\mathscr{L}$ qui ne satisfait pas F. Dans le modèle principal $\mathfrak{M}^*$ de $\mathscr{U}$ associé à $\mathfrak{M}^\tau$, F^* n'est pas satisfaite. Donc $\mathscr{U} \to F^*$ n'est pas un théorème d'ordre (0) de $\mathscr{L}^*$.

Si $\mathscr{U} \to F^*$ n'est pas un théorème d'ordre (0) de $\mathscr{L}^*$, il existe un modèle principal $\mathfrak{M}^*$ de $\mathscr{U}$ qui ne satisfait pas F^*. La réalisation $\mathfrak{M}^\tau$ d'ordre τ de $\mathscr{L}$ associée à $\mathfrak{M}^*$ est principale et ne satisfait pas F^*. Donc F n'est pas un théorème d'ordre τ. C. q. f. d.

Pour tout entier n, les formules dont les variables ont un rang $< n$ (p. 103) seront appelées formules d'ordre n.

Réduction d'une certaine classe de formules du second ordre.

Soit A une formule de $\mathscr{L}^\tau$ dont les variables libres, soient $x_1, ..., x_n$, ont le type ou bien d'individu ou bien de relation entre individus $(\sigma_1, ..., \sigma_p)$ où $\sigma_i = 0$ pour $(1 \leqslant i \leqslant p)$, type qui sera désigné par (p). Soit $\mathscr{L}_m$ $(m \leqslant n)$ le langage du premier ordre obtenu en ajoutant à $\mathscr{L}$ les symboles s_i $(i \leqslant m)$ ne figurant pas dans $\mathscr{L}$, s_i de même type que x_i. Pour plus de clarté on écrit c_i' pour s_i si x_i est de type 0, et R_i' (symbole relationnel à p_i variables) si x_i est de type (p_i). Toute réalisation $\mathfrak{M}_m$ de $\mathscr{L}_m$ induit une réalisation $\mathfrak{M}$ de $\mathscr{L}$ (la restriction de $\mathfrak{M}_m$ au langage $\mathscr{L}$) ; $\mathfrak{M}_m = \mathfrak{M} \cup \{ \bar{s}_i : i \leqslant m \}$, où s_i est élément de l'ensemble de base de $\mathfrak{M}$ si $s_i = c_i'$ et élément de l'ensemble $E_{(p_i)}$ de base de $\mathfrak{M}^\tau$ de type (p_i) si $s_i = R_i' : \bar{s}_i \in E_{(p_i)}$ parce que *tout* sous-ensemble de E_{p_i} appartient à l'ensemble de base du type (p_i) du modèle principal.

A est dite *réductible* à la classe $\mathscr{A}$ des formules de $\mathscr{L}_m$ si, pour toute réalisation $\mathfrak{M} \cup \{ \bar{s}_i : i \leqslant m \}$, $\{ \bar{s}_i : i \leqslant m \}$ satisfait A dans $\mathfrak{M}^\tau$ si et seulement si $\mathfrak{M}_m$ satisfait toute formule de $\mathscr{A}$ ($\mathfrak{M}_m$ est modèle de $\mathscr{A}$).

LEMME 1. — *Toute formule* $\bigwedge x_{i+1} ... \bigwedge x_n\, A_n$ *de* $\mathscr{L}^\tau$, A_n sans *quantificateur est réductible à une (seule) formule prénexe* A_i^0 *de* $\mathscr{L}_i$ *dont tous les quantificateurs sont universels et toute formule de* $\mathscr{L}_n$ *est réductible à une (seule) formule de* $\mathscr{L}^\tau$. (A_n^0 sera appelée traduction canonique de A_n.)

Démonstration. — La formule A_n, étant sans quantificateur, est une formule propositionnelle construite sur des formules atomiques de $\mathscr{L}$ et sur des formules $(t_1, ..., t_{p_i})\ \varepsilon_{(p_i)} x_i$ $(1 \leqslant i \leqslant n,\ x_i$ de type $(p_i))$. A_n^0 est la formule obtenue en remplaçant d'abord x_i par c_i' si x_i est de type 0 et ensuite $(t_1, ..., t_{p_i})\ \varepsilon_{(p_i)}\ x_i$ par $R_i'(t_1, ..., t_{p_i})$. Toute formule atomique B de A_n est évidemment réductible à B^0, et les opérations propositionnelles préservent la réductibilité. Inversement toute formule sans quantificateur de $\mathscr{L}_n$ est réductible à la formule de $\mathscr{L}^\tau$ obtenue en remplaçant d'abord c_i' par x_i ; et $R_i'(t_1, ..., t_{p_i})$ par $(t_1, ..., t_{p_i})\ \varepsilon_{(p_i)}\ x_i$. La quantification de $\mathscr{L}_n$ préserve la réductibilité parce que les variables (d'individu) varient sur le même ensemble de base dans $\mathfrak{M}$ et $\mathfrak{M}_n$.

Supposons que $\bigwedge x_{i+2} ... \bigwedge x_n\ A_n$ soit réductible à A_{i+1}^0. Alors $\mathfrak{M} \cup (\bar{s}_j : j \leqslant i)$ satisfait $\bigwedge x_{i+1} ... \bigwedge x_n\ A_n$ si et seulement si, pour *toute* valeur s_{i+1}^* dans $\mathfrak{M}$ de même type que x_{i+1}, $\mathfrak{M} \cup \{ \bar{s}_j : j \leqslant i \} \cup \{ \bar{s}_{i+1}^* \}$ satisfait A_{i+1}^0. On distingue entre deux cas :

1° x_{i+1} est de type 0 et donc $s_{i+1} = c_{i+1}'$. Dans ce cas $\bigwedge x_{i+1} ... \bigwedge x_n\ A_n$ équivaut à $\bigwedge x_{i+1}'\ A_{i+1}'$, où A_{i+1}' résulte de A_{i+1}^0 en remplaçant c_{i+1}' par x_{i+1}'. $\bigwedge x_{i+1}'\ A_{i+1}'$ est évidemment une formule prénexe universelle de $\mathscr{L}_i$.

2° x_{i+1} est de type (p_{i+1}). Soit $A_{i+1}^0 = \bigwedge u_1 ... \bigwedge u_l\ X_1$, X_1 sans quantificateur. Soit b l'ensemble des termes qui apparaissent dans X_1 et soient $\bar{u}_1, ..., \bar{u}_l$, des éléments de E_0. Il est évident que s'il existe $\overline{R}_{i+1}'$ telle que

$$\mathfrak{M} \cup \{ \bar{s}_j : j \leqslant i \} \cup \{ \overline{R}_{i+1}', \bar{u}_1, ..., \bar{u}_l \}$$

satisfait $\neg\ X_1$, alors sa restriction à l'ensemble fini $\{ \bar{t} : t \in b \}$ satisfait aussi $\neg\ X_1$. Soit X_2 la conjonction des formules

$$t_1 = t_1' \wedge \cdots \wedge t_q = t_q' \wedge S(t_1, ..., t_q) \rightarrow S(t_1', ..., t_q')$$

obtenues pour tout symbole relationnel S de $\mathscr{L}_{i+1}$, S à q variables, et pour tout 2 q-uplet de termes de l'ensemble b, et soit $D_1, ..., D_r$ une liste de tous les diagrammes sur b dans le langage $\mathscr{L}_i$. Si X_3 est la disjonction des $D_s (1 \leqslant s \leqslant r)$ tels que $X_2 \wedge \neg\ X_1 \wedge D_s$ soit contradictoire, alors $\bigwedge u_1 ... u_l\ X_3$ est la formule cherchée : si la structure $\mathfrak{M} \cup \{ \bar{s}_j : j \leqslant i \}$ la satisfait, alors pour tout b-uplet $\bar{u}_1, ..., \bar{u}_l$, elle satisfait un de ces diagrammes et, par conséquent, il n'existe aucune $\overline{R}_{i+1}'$ telle que $\mathfrak{M} \cup \{ \bar{s}_j : j \leqslant i \} \cup \{ \overline{R}_{i+1}' \}$ satisfasse $\bigvee u_1 ... \bigvee u_l \neg\ X_1$. Dans le cas contraire, il existe $\bar{u}_1, ..., \bar{u}_l$ tels que $\mathfrak{M} \cup \{ \bar{s}\ : j \leqslant i \}$ satisfait $\neg\ X_3$, et par conséquent un diagramme D_s tel que $X_2 \wedge \neg\ X_1^* \wedge D_s$ a un modèle ; autrement dit, il existe une $\overline{R}_{i+1}'$ telle que

$$\{ \bar{s}_j : j \leqslant i \} \cup \{ R_{i+1}', \bar{u}_1, ..., \bar{u}_l \}$$

satisfait $\neg\ X_1$.

THÉORÈME 2. — *Soit* $A = Q_1\ x_1 ... Q_n\ x_n\ A_n$ *une formule close prénexe de* $\mathscr{L}^\tau$,

A_n sans quantificateur, x_i de type (p_i) si $Q_i = \vee$, x_i ou bien de type 0 ou bien de type (p_i) si $Q_i = \wedge$. Alors A est réductible à un ensemble $\mathscr{A}$ de formules prénexes closes de $\mathscr{L}$ dont tous les quantificateurs sont universels. ($\mathfrak{M}^r$ *est modèle de A si et seulement si $\mathfrak{M}$ est modèle de $\mathscr{A}$.*)

Démonstration par récurrence sur le nombre n de quantificateurs : on pose

$$A_i = Q_{i+1}\, x_{i+1} \dots Q_n\, x_n\, A_n$$

et on démontre que A_i est réductible à un ensemble $\mathscr{A}_i$ de formules (prénexes) universelles de $\mathscr{L}_i$.

D'après le lemme 1, A_n est réductible à un tel ensemble $\mathscr{A}_n$ (qui se réduit à une seule formule). Supposons A_{i+1} réductible à la classe $\mathscr{A}_{i+1}$ de formules de $\mathscr{L}_{i+1}$.

Si $Q_{i+1} = \vee$, le type de x_{i+1} est (p_{i+1}) et $\{ \bar{s}_j : j \leqslant i \}$ satisfait donc A_i dans $\mathfrak{M}^r$ si et seulement si il existe $\bar{s}^*_{i+1} \in E_{(p_{i+1})}$ tel que $\{ \bar{s}_j : j \leqslant i \} \cup \{ \bar{s}^*_{i+1} \}$ satisfasse A_{i+1}, ce qui équivaut, d'après l'hypothèse de récurrence, à l'existence d'un $\bar{s}^*_{i+1}$ tel que $\mathfrak{M} \cup \{ \bar{s}_j : j \leqslant i \} \cup \{ \bar{s}^*_{i+1} \}$ satisfasse toute formule de $\mathscr{A}_{i+1}$. Or, d'après le théorème de plongement (Chap. 3), la structure $\mathfrak{M} \cup \{ \bar{s}_j : j \leqslant i \}$ peut être plongée dans un modèle de $\mathscr{A}_{i+1}$ si et seulement si elle satisfait l'ensemble $\mathscr{A}_i$ des formules universelles de $\mathscr{L}_i$ qui sont conséquences de $\mathscr{A}_{i+1}$. Par conséquent, A_i est réductible à cet ensemble $\mathscr{A}_i$.

Si $Q_{i+1} = \wedge$, d'après l'hypothèse de récurrence, $\{ \bar{s}_j : j \leqslant i \}$ satisfait A_i dans $\mathfrak{M}^r$ si et seulement si, pour toute valeur $\bar{s}^*_{i+1}$ dans $\mathfrak{M}^r$, de même type que x_{i+1}, $\mathfrak{M} \cup \{ \bar{s}_j : j \leqslant i \} \cup \{ \bar{s}^*_{i+1} \}$ satisfait A^0_{i+1}. On applique le lemme 1. (Pour une généralisation, voir exercice 2.)

Formules infinies définissant des relations à un nombre fini d'arguments.

Soit $A_i (i \in I)$ une famille de formules de $\mathscr{L}$ ayant leurs variables libres prises parmi $x_1, \dots, x_p$. Considérons une réalisation $\mathfrak{M}$ de $\mathscr{L}$ et soit $\overline{A_i}$ la valeur prise par A_i dans $\mathfrak{M}$. Nous dirons que $\mathfrak{M}$ *satisfait la formule infinie* $\vee x_1 \dots \vee x_p \bigwedge_i A_i$ si et seulement si $\bigcap_{i \in I} \overline{A_i} \neq \phi$. Si $\bigcap_{i \in I} \overline{A_i} = \phi$ nous dirons que $\mathfrak{M}$ satisfait la formule infinie $\wedge x_1 \dots \wedge x_p \bigvee_i \neg A_i$, dite négation de la précédente. Nous n'étudions pas par la suite l'itération générale des opérations propositionnelles ci-dessus (conjonction infinie $\bigwedge$, disjonction infinie $\bigvee$ et négation). Les deux types de formules décrits ici nous serviront à définir quelques classes de structures, classes qui ne sont définissables par aucun ensemble de formules finies du premier ordre (exercice 5).

On considérera des langages à plusieurs types de variables. Supposons le langage $\mathscr{L}$ égalitaire et soient $\mathfrak{M}$ un modèle de $\mathscr{E}_{\mathscr{L}}$, $\mathfrak{M}'$ la réalisation égalitaire qu'on en déduit par passage au quotient. Nous avons vu que $\mathfrak{M}$ et $\mathfrak{M}'$ satis-

font les mêmes formules closes de $\mathscr{L}$. En fait $\mathfrak{M}$ *et* $\mathfrak{M}'$ *satisfont aussi les mêmes formules infinies de* $\mathscr{L}$: soit en effet

$$\forall x_1 \ldots \forall x_p \bigwedge_i A_i(x_1, \ldots, x_p)$$

une formule infinie et soient $\overline{A}_i$ et $\overline{\overline{A}}_i$ les valeurs prises par la formule $A_i(x_1, \ldots, x_p)$ respectivement dans $\mathfrak{M}$ et $\mathfrak{M}'$. On a $\overline{\overline{A}}_i = \overline{A}_i/\overline{E}$, $\overline{A}_i$ étant saturée pour la relation d'équivalence $\overline{E}$. Il en résulte que

$$\bigcap_i \overline{\overline{A}}_i = \bigcap_i \overline{A}_i/\overline{E}\,;$$

donc $\bigcap_i \overline{A}_i$ et $\bigcap_i \overline{\overline{A}}_i$ sont simultanément vides ou non vides.

LEMME 2. — *Soit* $\mathscr{A}$ *un ensemble consistant de formules finies closes de* $\mathscr{L}$ *et* $\mathscr{A}_i$ $(i < \lambda)$ *une famille d'ensembles de formules finies closes de* $\mathscr{L}$. *Si tout modèle de* $\mathscr{A}$ *satisfait un des ensembles* $\mathscr{A}_i$, *il existe un ensemble* $\mathscr{B}$ *de formules finies closes de* $\mathscr{L}$ *et un ordinal* $j < \lambda$, *tels que* card $\mathscr{B}$ < card λ (*et* card $\mathscr{B} \leqslant$ card $\mathscr{L}$), *que* $\mathscr{A} \cup \mathscr{B}$ *soit consistant, et que* $\mathscr{A}_j$ *soit conséquence de* $\mathscr{A} \cup \mathscr{B}$ (la notation card X désigne le cardinal de l'ensemble X).

Démonstration (en utilisant le corollaire du théorème de finitude, Chap. 5). — On peut évidemment supposer que λ est un cardinal. Soit $\mathscr{A}_0^+ = \mathscr{A}$. Pour $j \geqslant 0$ on a deux cas :

1° S'il existe $k \leqslant j$ tel que $\mathscr{A}_k$ soit conséquence de $\bigcup_{i<k} \mathscr{A}_i^+$ on pose $\mathscr{A}_j^+ = \bigcup_{i<k} \mathscr{A}_i^+$ (c'est-à-dire la suite $\mathscr{A}_j^+ = \mathscr{A}_k^+$ pour $j \geqslant k$).

2° Dans le cas contraire, on pose $\mathscr{A}_j^+ = \bigcup_{i<j} \mathscr{A}_i^+ \cup \{\neg A_j^*\}$, où $A_j^* \in \mathscr{A}_j$ et n'est pas conséquence de $\bigcup_{i<j} \mathscr{A}_i^+$.

Il existe un j_0 $(j_0 < \lambda)$ tel que le cas 1° s'applique, sinon $\bigcup_{j<\lambda} \mathscr{A}_j^+$ aurait un modèle de $\mathscr{A}$ ne satisfaisant aucun $\mathscr{A}_j$, parce que ne satisfaisant pas A_j^* $(j < \lambda)$. On prend $\mathscr{B} = \{\neg A_i^* : i < j_0\}$.

Evidemment card $\mathscr{B} \leqslant$ card $\mathscr{L}$ parce qu'il n'existe que card $\mathscr{L}$ formules de $\mathscr{L}$ (il existe plus de card $\mathscr{L}$ ensembles de formules de $\mathscr{L}$ non équivalents).

THÉORÈME 3. — *Soit* J *un ensemble de formules infinies du langage égalitaire* $\mathscr{L}$, *du type* $\forall x_1 \ldots \forall x_n \bigwedge_\lambda A_\lambda^j(x_1, \ldots, x_n)$ $(\lambda < \Lambda = \text{card}\,\mathscr{L},\ j \in J)$, *et soit* $\mathscr{A}$ *un ensemble de formules de* $\mathscr{L}$, *ayant un modèle égalitaire, et tel que tout modèle égalitaire de* $\mathscr{A}$ *satisfasse une des formules infinies de* J. *Alors il existe une formule infinie de* J, *soit*

$$\forall x_1 \ldots \forall x_n \bigwedge_\lambda A_\lambda(x_1, \ldots, x_n) \ (\lambda < \Lambda)$$

et une famille $F_i(x_1, ..., x_n)$ $(i \in I)$ de formules de $\mathscr{L}$ telles que

$$\text{card}\, I < \text{card}\, J \times \text{card}\, \mathscr{L}, \quad \text{et} \quad \text{card}\, I \leqslant \text{card}\, \mathscr{L}\ ;$$

$(\mathscr{A}, \bigvee x_1 \dots \bigvee x_n \bigwedge\!\!\!\bigwedge_i F_i(x_1, ..., x_n))$ a un modèle égalitaire ;
pour tout $\lambda < \Lambda$ il existe $i \in I$ tel que $\mathscr{A} \vdash \bigwedge x_1 \dots \bigwedge x_n[F_i \to A_\lambda]$.

Démonstration. — On utilisera les modèles canoniques du chapitre 5. Puisqu'il s'agit d'un langage égalitaire on suppose $\mathscr{E}_{\mathscr{L}} \subset \mathscr{A}$; par conséquent, tout modèle (égalitaire ou non) de $\mathscr{A}$ satisfait une des formules infinies de J. Tout modèle canonique de $(\mathscr{A}, \Omega)$ satisfait une des formules infinies de J, donc satisfait un des ensembles $\{ A^j_\lambda(a_1, ..., a_n) \}$ $(\lambda < \Lambda)$ pour $a_1, ..., a_n \in \Delta$, de mêmes types respectifs que $x_1, ..., x_n$. Or cette famille d'ensembles a pour cardinal card $J \times$ card $\mathscr{L}$. D'après le lemme 2, il existe une famille $(B_i)_{i \in I}$ de formules de $\mathscr{L}_\Delta$ telle que card $I \leqslant$ card $\mathscr{L}$ et card $I <$ card $\mathscr{L} \times$ card J, et un ensemble $\{ A^j_\lambda(a_1, ..., a_n) \}$ $(\lambda < \Lambda)$ tels que $(\mathscr{A}, \Omega) \cup (B_i)_{i \in I}$ possède un modèle et a pour conséquence $A^j_\lambda(a_1, ..., a_n)$, pour tout $\lambda < \Lambda$. (card $I \leqslant$ card $\mathscr{L}$ parce qu'il n'existe que card $\mathscr{L}$ formules différentes dans $\mathscr{L}$). Pour chaque $\lambda < \Lambda$ il existe donc un sous-ensemble fini de $\{ B_i \}_{i \in I}$, dont nous désignerons la conjonction par B, et un sous-ensemble fini de $\mathscr{A}$, dont nous désignerons la conjonction par A, tels que

$$\Omega \vdash A \wedge B \to A^j_\lambda(a_1, ..., a_n)\,.$$

Si $b_1, ..., b_p$ sont les éléments de Δ qui apparaissent dans B, on a donc

$$\theta_{a_1} \wedge \cdots \wedge \theta_{a_n} \wedge \theta_{b_1} \wedge \cdots \wedge \theta_{b_p} \vdash A \wedge B \to A^j_\lambda(a_1, ..., a_n)\,.$$

Donc

$$A \vdash \theta_{a_1} \wedge \cdots \wedge \theta_{a_n} \wedge \theta_{b_1} \wedge \cdots \wedge \theta_{b_p} \wedge B \to A^j_\lambda(a_1, ..., a_n)$$

d'après le lemme 6, chapitre 5.

On pose

$$F_j(a_1, ..., a_n) = \theta_{a_1} \wedge \cdots \wedge \theta_{a_n} \wedge \theta_{b_1} \wedge \cdots \wedge \theta_{b_p} \wedge B\,.$$

L'indice parcourt un ensemble dont le cardinal est inférieur ou égal au cardinal de l'ensemble des parties finies de I. La famille $F_j(x_1, ..., x_n)$ a donc les propriétés voulues.

COROLLAIRE. — *Si, dans l'énoncé du théorème, $\mathscr{L}$ et J sont supposés dénombrables (donc $\Lambda = \omega$), il existe une formule* finie *$B(x_1, ..., x_n)$ telle que : $\mathscr{A}, \bigvee x_1 \dots \bigvee x_n\, B(x_1, ..., x_n)$ a un modèle égalitaire et, pour tout entier p,*

$$\mathscr{A} \vdash \bigwedge x_1 \dots \bigwedge x_n[B(x_1, ..., x_n) \to A_p(x_1, ..., x_n)]\,.$$

Langages dénombrables ; ensembles dénombrables de formules infinies. L'ensemble des variables, symboles relationnels, symboles de constantes du langage $\mathscr{L}$ considéré est dénombrable.

THÉORÈME 4. — *Soit $\mathscr{A}$ un ensemble de formules closes finies de $\mathscr{L}$ et J un ensemble dénombrable de formules infinies du type*

$$\Lambda x_1 \dots \Lambda x_p \bigvee_n A_n^j(x_1, \dots, x_p) \qquad (j = 1, 2, \dots ; \; p = p(j)) .$$

L'ensemble des formules finies de $\mathscr{L}$ satisfaites par tout modèle de $\mathscr{A} \cup J$ est le plus petit ensemble $\mathscr{A}^J$ de formules finies de $\mathscr{L}$ tel que :

1° *Si G est une formule close de $\mathscr{L}$ et si $\mathscr{A}^J \vdash G$, alors $G \in \mathscr{A}^J$.*

2° *Si $G(x_1, \dots, x_p)$, est une formule de $\mathscr{L}$ telle que*

$$\mathscr{A}^J \vdash \Lambda x_1 \dots \Lambda x_p[A_n^j(x_1, \dots, x_p) \to G(x_1, \dots, x_p)]$$

pour un certain entier j, et pour tout n, alors $\Lambda x_1 \dots \Lambda x_p \, G(x_1, \dots, x_p) \in \mathscr{A}^J$.

(L'énoncé serait faux sans la restriction au cas dénombrable ; voir exercice 3.)

Démonstration. — Il est immédiat que l'ensemble des formules qui sont satisfaites par tous les modèles de $\mathscr{A} \cup J$ contient $\mathscr{A}^J$.

Inversement, soit F une formule satisfaite par tous les modèles de $\mathscr{A} \cup J$. Si $\mathscr{A}^J \cup (\neg F)$ n'a pas de modèle égalitaire, F est conséquence égalitaire de A^J et donc $F \in \mathscr{A}^J$. Si $\mathscr{A}^J \cup (\neg F)$ a un modèle égalitaire, par hypothèse il satisfait la négation d'une des formules de J, soit

$$\vee x_1 \dots \vee x_p \bigwedge_n \neg A_n^{j_0}(x_1, \dots, x_p) ,$$

et, d'après le théorème 3 il existe une formule $G(x_1, \dots, x_p)$ telle que $\mathscr{A}^J \cup \{ \neg F, \vee x_1 \dots \vee x_p \, G(x_1, \dots, x_p) \}$ ait un modèle (égalitaire) et telle que, pour chaque entier n, on ait

$$\mathscr{A}^J \cup \{ \neg F \} \vdash \Lambda x_1 \dots \Lambda x_p[G(x_1, \dots, x_p) \to \neg A_n^{j_0}(x_1 \dots, x_p)]$$

et par conséquent $\mathscr{A}^J \cup \{ \neg F \} \vdash$

$$\Lambda x_1 \dots \Lambda x_p[A_n^{j_0}(x_1, \dots, x_p) \to \neg G(x_1, \dots, x_p)] .$$

Dans ce cas

$$\mathscr{A}^J \vdash \Lambda x_1 \dots \Lambda x_p[A_n^{j_0}(x_1, \dots, x_p) \to (F \vee \neg G(x_1, \dots, x_p))] .$$

Par hypothèse

$$\Lambda x_1 \dots \Lambda x_p(F \vee \neg G(x_1, \dots, x_p)) \in \mathscr{A}^J .$$

Puisque F est une formule close, $F \vee \Lambda x_1 \dots \Lambda x_p \neg G(x_1, \dots, x_p)$ est conséquence de $\mathscr{A}^J$ et, par conséquent, élément de $\mathscr{A}^J$; donc

$$\mathscr{A}^J \cup \{ \neg F, \vee x_1 \dots x_p \, G(x_1, \dots, x_p) \}$$

n'a pas de modèle. Par conséquent, $\mathscr{A}^J \cup \{ \neg F \}$ n'a pas de modèle et par suite $\mathscr{A}^J \vdash F$.

COROLLAIRE. — *Pour que $\mathscr{A} \cup J$ ait un modèle, il faut et il suffit que A^J ait un modèle.*

En effet si $\mathscr{A} \cup J$ a un modèle celui-ci est un modèle de $\mathscr{A}^J$. Si $\mathscr{A} \cup J$ n'a pas de modèle, la formule finie $\perp$ est satisfaite par tous les modèles de $\mathscr{A} \cup J$, donc $\perp \in \mathscr{A}^J$ et $\mathscr{A}^J$ n'a pas de modèle.

EXERCICES

1. *a*) Trouver des formules du second ordre dont les classes de modèles principaux soient respectivement : (i) les bons ordres, (ii) les bons ordres d'ordinal ω, (iii) les ordres complets, (iv) les ordres denses complets, sans premier ni dernier élément tels qu'il existe un sous-ensemble dénombrable (de l'ensemble de base) dense sur l'ensemble de base.

b) Montrer que les classes (ii) et (iv) définies dans *a*) contiennent un seul élément à un isomorphisme près.

Solution.

Soit $\mathscr{L}$ le langage égalitaire du premier ordre contenant un seul symbole relationnel à 2 variables que nous notons $<$, soient X, Y, Z des variables de type (0) et soit U une variable de type (0, 0). Le rang de chacune de ces variables est 1. Soit O la formule de $\mathscr{L}$ qui est la conjonction des axiomes d'ordre strict. On écrira Xx pour $x \epsilon X$ (p. 133).

a) (i) La formule

$$O \wedge \bigwedge X \{ \bigvee x Xx \to \bigvee y [Xy \wedge \bigwedge z (z < y \to \neg Xz)]\} .$$

de $\mathscr{L}^{(o)}$ — appelons-la B —, exprime que tout sous-ensemble X non vide ($\bigvee x Xx$) a un premier élément, c'est-à-dire que l'ordre $<$ est un bon ordre (cf. Ex. 7 du Chap. 3).

(ii) $B \wedge \bigwedge x [\bigwedge z \neg (z < x) \vee \bigvee y \bigwedge z (z < x \leftrightarrow z = y \vee z < y)]$

est la formule cherchée.

(iii) La formule

$$\bigwedge x \bigwedge y ((Xx \wedge y < x) \to Xy) \wedge \bigvee x Xx \wedge \bigvee x \neg Xx \wedge$$
$$\wedge \bigwedge x \bigvee y [Xx \to (x < y \wedge Xy)]$$

de $\mathscr{L}^{(o)}$, — appelons-la $C(X)$ —, exprime que X est une coupure ouverte à droite. Alors, les ordres complets sont les modèles de la formule

$$O \wedge \bigwedge X \bigvee x \bigwedge y [C(X) \to (Xy \leftrightarrow y < x)] ,$$

que nous désignerons par Com.

(iv) Soient $D(Y)$ la formule $\bigwedge x \bigwedge y[x < y \rightarrow \bigvee z(x < z \wedge z < y \wedge Yz)]$ de $\mathscr{L}^{(0)}$ (Y est dense sur l'ensemble de base relativement à l'ordre $<$), $W(Z)$ la formule de $\mathscr{L}^{(0)}$ qui exprime que la restriction de $<$ à l'ensemble Z est un bon ordre d'ordinal ω, et $I(U, Y, Z)$ la formule qui exprime que U est le graphe d'un isomorphisme entre Y et Z :

$$\bigwedge x \bigvee y \bigwedge z(Yx \rightarrow (Zy \wedge [U(x, z) \leftrightarrow y = z]) \wedge \\ \wedge \bigwedge y \bigvee x \bigwedge z(Zy \rightarrow (Yx \wedge [U(z, y) \leftrightarrow x = z]) \wedge \\ \wedge \bigwedge x \bigwedge y[U(x, y) \rightarrow (Yx \wedge Zy)] .$$

Alors la formule cherchée est :

$$\bigwedge x \bigvee y(y < x) \wedge \bigwedge x \bigvee y(x < y) \wedge \text{Com} \wedge \\ \wedge \bigvee Y \bigvee Z \bigvee U[D(Y) \wedge W(Z) \wedge I(U, Y, Z)].$$

b) Il est évident que les bons ordres d'ordinal ω sont tous isomorphes à l'ordre naturel des entiers positifs. D'après l'exercice 3, chapitre 4, tout ordre dense dénombrable sans premier ni dernier élément est isomorphe à l'ordre naturel des rationnels. Par conséquent, tout élément de la classe (iv) est isomorphe à l'ordre naturel sur les réels.

2. Soit $\mathscr{L}'_m$ le langage obtenu en ajoutant au langage $\mathscr{L}$, pour $i \leqslant m$, un symbole d'individu $c'_i (i \in I)$, un symbole relationnel à p_i variables $(i \in R)$, ou bien un symbole fonctionnel f_i à $p_i - 1$ variables $(i \in F)$; on suppose $F = \{ n_1, ..., n_k \} (n_i < n_{i+1}, i < k)$. Soit $\mathscr{L}_m$ le langage obtenu à partir de $\mathscr{L}'_m$ en remplaçant tout f_i par $R_i (i \in F)$, symbole relationnel à p_i variables. Pour $j \leqslant k$ on écrit F_j pour $(q_j = p_{n_j})$

$$\bigwedge u_1 \ldots \bigwedge u_{p_j - 1} \bigvee u_{q_j} R_{q_j}(u_1, ..., u_{p_j}) \wedge \bigwedge u_1 \ldots \bigwedge u_{q_j - 1} \bigwedge v \bigwedge w \\ [R(u_1, ..., u_{q_j - 1}, v) \wedge R(u_1, ..., u_{q_j - 1}, w) \rightarrow v = w] .$$

a) Pour toute formule A' de $\mathscr{L}'_m$ sans quantificateur, trouver une formule A^o prénexe purement universelle de $\mathscr{L}_m$ telle que, pour toute réalisation $\mathfrak{M}$ de $\mathscr{L}$, pour toute suite $\bar{c}'_i$ d'éléments de l'ensemble E_0 de base de $\mathfrak{M}(i \in I)$, $\bar{R}'_i \subset E_0^{p_i}(i \in R)$, $\bar{f}_i : E_0^{p_i - 1} \rightarrow E_0(i \in F)$, $\bar{R}'_i \subset E^{p_i}$, $\bar{R}'$ étant le graphe de $\bar{f}'_i$,

$$\mathfrak{M} \cup \{ \bar{c}'_i : i \in I \} \cup \{ \bar{R}'_i : i \in R \} \cup \{ \bar{f}_i : i \in F \}$$

satisfait A' si et seulement si $\mathfrak{M} \cup \{ \bar{c}'_i : i \in I \} \cup \{ \bar{R}'_i : i \in R \cup F \}$ satisfait A^0.

b) Soit A' une formule de $\mathscr{L}'_n$ sans quantificateur, A^0 la formule

correspondante de $\mathscr{L}_n$ trouvée dans (*a*) et soit A_n la traduction de $F_1 \wedge \cdots \wedge F_k \to A^0$ dans $\mathscr{L}^\tau$ d'après le lemme 1. Montrer que $Q_1 x_1 \ldots Q_n x_n A_n$ est réductible à une classe de formules prénexes universelles de $\mathscr{L}$, si $Q_i = \bigwedge$ pour tout $i \in F$.

c) $\mathscr{L}$ est le langage à un seul symbole relationnel P à une seule variable. Montrer qu'il n'existe aucun ensemble $\mathscr{A}$ de formules de $\mathscr{L}$ tel que la réalisation $\langle E, \bar{P} \rangle$ puisse être complétée en une réalisation $(E, \bar{P}, \bar{f})$ $(f \in E^E)$ qui satisfait

$$\bigwedge x(f(fx) = x \wedge Px \leftrightarrow \neg P(fx))$$

si et seulement si $\langle E, \bar{P} \rangle$ satisfait $\mathscr{A}$.

d) Déduire de *c*) qu'il existe une formule close $\bigvee x_1 \bigvee x_2 \bigvee x_3 \bigwedge x_4 A$ de $\mathscr{L}^{(0)}$, A sans quantificateur, x_1 de type (0, 0), x_2, x_3, x_4 de type 0 qui n'est réductible à aucun ensemble de formules de $\mathscr{L}$.

Solution.

a) Soit T la plus petite classe de termes de $\mathscr{L}'_m$ qui contient tout terme qui apparaît dans A', et telle que $t_1, \ldots, t_{p_i-1} \in T$ si $f_i(t_1, \ldots, t_{p_i-1}) \in T (i = n_1, \ldots, n_k)$. Pour tout terme $t \in T$, le degré d'une constante $= 0$ et le degré de $t = 1 + \max$ degrés t_j $(j < p_i)$. Pour t de degré > 0, soit y_t une variable d'individu distincte de tous les symboles de A' et soient y_t et $y_{t'}$ distinctes pour $t \neq t'$. On arrange les y_t selon le degré de t. Pour tout $t = f_i(t_1, \ldots, t_{p_i-1})$, $t \in T$, soit R_t la formule $R_i(t_1^*, \ldots, t_{p_i-1}^*, y_t)$, où $t_j^* = y_{t_j}$ si degré $t_j > 0$, $t_j^* = t_j$ si degré $(t_j) = 0$ $(j < p_i)$. Soit B la conjonction de toutes les formules R_t (degré de $t > 0$, $t \in T$). La formule $\bigwedge y_{t1} \ldots \bigwedge y_{ts} (B \to A^1)$ est la formule cherchée, où $t_1, \ldots, t_s$ est une liste des termes de T de degré < 0, et A^1 est obtenue en remplaçant chacun de ces t par y_t dans A'.

b) Soit $A_i = Q_{i+1} x_{i+1} \cdots Q_n x_n(F_j \wedge \cdots \wedge F_k \to A)$, où $n_j \geqslant i + 1$ et $n_{j-1} < i$. On va montrer que A_i est *réductible* à une classe $\mathscr{A}_i$ de formules prénexes universelles de $\mathscr{L}_i$, au sens suivant :

$$\mathfrak{M} \cup \{ \bar{c}'_h : h \leqslant i, i \in I \} \cup \{ \bar{R}'_h : h \in R, h \leqslant i \} \cup \{ \bar{f}'_h : h \in F, h \leqslant i \},$$

soit $\mathfrak{M}_i$, est modèle de $\mathscr{A}_i$ si et seulement si

$$\mathfrak{M} \cup \{ \bar{c}'_h : h \leqslant i, i \in I \} \cup \{ \bar{R}'_h : h \in R \cup F, h \leqslant i \}$$

satisfait A_i où, pour $h \in F$, $\bar{R}'_h$ est le graphe de $\bar{f}_h$. Pour $i = n$, c'est une conséquence du lemme 1 et de (*a*).

Supposons que A_{i+1} est réductible à la classe $\mathscr{A}_{i+1}$ de formules prénexes universelles de $\mathscr{L}_{i+1}$. Si $i + 1 \neq n_j$, on applique le théorème en

tenant compte du fait que le théorème de plongement est valide pour les langages avec symboles fonctionnels.

Si $i + 1 = n_j$, $Q_{i+1} = \wedge$. Soit X, $X \in \mathscr{A}_{i+1}$, $= \wedge u_1 \dots \wedge u_l\, X_1$, X_1 sans quantificateur. Soit T l'ensemble des termes construit à partir des termes qui apparaissent dans X (comme dans a)). Pour tout $t \in T$ on associe t^* suivant le degré : si deg $t = 0$, $t^* = t$; si $t = f_{n_h}(t_1, \dots, t_q)$ $(q = p_{n_h} - 1)$ et $h \neq j$, $t^* = f_{n_h}(t_1^*, \dots, t_q^*)$, et si $h = j$, $t^* = y_t$, où y_t est une variable distincte de tous les symboles figurant dans X ; soient y_t, $y_{t'}$ distinctes pour t distinct de t'. Soient $\bar{u}_1, \dots, \bar{u}_l$ des éléments de l'ensemble de base de $\mathfrak{M}$. Il est évident que si une fonction $\bar{f}_{i+1}$ est telle que $\mathfrak{M}_i \cup \{ \bar{f}_{i+1}, \bar{u}_1, \dots, \bar{u}_l \}$ satisfait $\neg X_1$, il en est de même pour $\bar{f}_{i+1}^*$ si $\bar{f}_{i+1}$ et $\bar{f}_{i+1}^*$ prennent les mêmes valeurs sur $\{ \bar{t} : t \in T \}$. Soit X_1^* la formule obtenue à partir de X_1 en remplaçant t par t^* et soit X_2 la conjonction de toutes les formules $(q = p_{i+1} - 1)$

$$t_1^* = s_1^* \wedge \cdots \wedge t_q^* = s_q^* \rightarrow y_t = y_s ,$$

où s, $t \in T$, $t = f_{i+1}(t_1, \dots, t_q)$, $s = f_{i+1}(s_1, \dots, s_q)$. Pour qu'il existe $\bar{f}_{i+1}$ telle que $\mathfrak{M}_i \cup \{\bar{f}_{i+1}\}$ satisfasse X_1 il faut et il suffit que $\mathfrak{M}_i$ satisfasse

$$\wedge y_{t_1} \dots \wedge y_{t_r}(X_2 \rightarrow X_1^*) ,$$

où $y_{t_1}, \dots, y_{t_r}$ est une liste des variables introduites.

c) $< E, \bar{P} >$ $(\bar{P} \subset E)$ peut être complétée en un modèle de

$$\wedge x(ffx = x \wedge Px \leftrightarrow \neg Pfx)$$

si et seulement si $\bar{P}$ et $E - \bar{P}$ ont le même cardinal. Or, d'après l'élimination des quantificateurs (Ch. 4, anneaux booléens) pour toute formule X close de $\mathscr{L}$, ou bien X est vraie dans toute réalisation dans laquelle $\bar{P}$ et $E - \bar{P}$ sont tous deux infinis, ou bien X est fausse dans toute réalisation satisfaisant à cette condition. On prend E_0 non dénombrable, $\bar{P}_0$ dénombrable, E_1 dénombrable (et infini), $\bar{P}_1$ et $E_1 - \bar{P}_1$ dénombrables ; pour tout ensemble $\mathscr{A}$ de formules closes de $\mathscr{L}$ ou bien $\langle E_0, \bar{P}_0 \rangle$ et $\langle E_1, \bar{P}_1 \rangle$ sont deux modèles de $\mathscr{A}$ ou bien ni l'un ni l'autre n'en est un. Or $\langle E_1, \bar{P}_1 \rangle$ satisfait la formule ci-dessus, mais non $\langle E_0, \bar{P}_0 \rangle$.

d) $\langle E, \bar{P} \rangle$ peut être complétée en un modèle de $\wedge x(ffx = x \wedge Px \leftrightarrow \neg Pfx)$ si et seulement si elle peut être complétée en un modèle de

$$\wedge x \vee y \wedge z[(Bxz \leftrightarrow z = y) \wedge Byx \wedge (Px \leftrightarrow \neg Py)] .$$

On obtient la formule cherchée en appliquant le lemme 1.

3. *a*) Soit $\mathscr{A}$ un ensemble de formules finies de $\mathscr{L}$, J un ensemble de formules infinies de type

$$\wedge x_1 \dots \wedge x_p \bigvee_n A_n(x_1, \dots, x_p) \qquad (n = 1, 2, 3, \dots),$$

et $\mathscr{A}^J$ l'ensemble de formules défini dans l'énoncé du théorème 4. Montrer que pour que $F \in \mathscr{A}^J$ il faut et il suffit qu'il existe un sous-ensemble dénombrable $\mathscr{A}_1$ de $\mathscr{A}$ et un sous-ensemble dénombrable J_1 de J tels que $F \in \mathscr{A}_1^{J_1}$ ($\mathscr{A}$ n'est évidemment pas supposé dénombrable).

b) On suppose que $\mathscr{L}$ est le langage à une seule sorte de variable ainsi défini: $C_{\mathscr{L}} = \mathbf{N}$, $\mathrm{R}_{\mathscr{L}}^{(1)} = \{ R_\xi : \xi \in \mathfrak{P}(\mathbf{N})\} \cup \{ R \}$, où R (est un symbole quelconque qui) n'est ni dans $\mathbf{N}$ ni un R_ξ. Soit $\mathscr{A}$ l'ensemble des formules suivantes de $\mathscr{L}$

$$\{ R_\xi n : n \in \xi, \xi \in \mathfrak{P}(\mathbf{N}) \} \cup \{ \neg R_\xi n : n \notin \xi, \xi \in \mathfrak{P}(\mathbf{N}) \} \cup$$
$$\cup \{ \vee x(Rx \leftrightarrow \neg R_\xi x) : \xi \in \mathfrak{P}(\mathbf{N}) \},$$

et $J = \left\{ \wedge x \bigvee_n x = n \right\}$.

Montrer que $\mathscr{A} \cup J$ n'a pas de modèle, mais que tout sous-ensemble dénombrable en a un. En déduire que $\mathscr{A}^J$ n'est pas contradictoire.

c) On suppose que $\mathscr{L}$ est le langage ainsi défini : $C_{\mathscr{L}} = \mathbf{N}$, un seul symbole relationnel R, R ayant un seul argument. $\mathscr{A} = \phi$ et J est l'ensemble non dénombrable

$$\left\{ \wedge x \bigvee_n x = n \right\} \cup \left\{ \bigvee_n (\neg)^{\xi_n} Rn : \xi \in \mathfrak{P}(\mathbf{N}) \right\},$$

où $(\neg)^{\xi_n}$ désigne $\neg$ si $n \in \xi$, et $\neg\neg$ si $n \notin \xi$.

Montrer que $\mathscr{A} \cup J$ n'a pas de modèle, mais que chacun de ses sous-ensembles dénombrables en a un.

Solution.

a) Il suffit de montrer que toutes les conditions de clôture qu'on a imposées à l'ensemble $\mathscr{A}^J$ sont aussi satisfaites par la plus petite classe $\mathscr{A}^C$ de formules (finies) de $\mathscr{L}$ telle que : $\mathscr{A} \subset \mathscr{A}^C$; pour toute formule close G de $\mathscr{L}$, si $\mathscr{A}^C \vdash G$ est alors $G \in \mathscr{A}^C$; et, pour tout j et pour toute formule $G(x_1, \dots, x_p)$ $(p = p(j))$ s'il existe un sous-ensemble dénombrable $\mathscr{A}_0 \cup J_0$ de $\mathscr{A} \cup J$ tel que, pour tout n,

$$\wedge x_1 \dots \wedge x_p(A_n^j(x_1, \dots, x_p) \rightarrow G(x_1, \dots, x_p))$$

soit satisfaite dans tout modèle de $\mathscr{A}_0 \cup J_0$, alors

$$\wedge x_1 \dots \wedge x_p \; G(x_1, \dots, x_p) \in \mathscr{A}^C .$$

Car, si pour tout n, il existe $\mathscr{A}_n \cup J_n$, ($\mathscr{A}_n \cup J_n$ dénombrable) tel que

$$\mathscr{A}_n \cup J_n \vdash \bigwedge x_1 \dots x_p(A_n^j(x_1, \dots, x_p) \to G(x_1, \dots, x_p)),$$

alors on peut prendre pour $\mathscr{A}_0$ le sous-ensemble dénombrable $\bigcup_n (\mathscr{A}_n \cup J_n)$.

b) et c) sont évidentes en tenant compte du fait que tout modèle de $\bigwedge x \bigvee_n (x = n)$ admet forcément comme réalisation de R l'un des ensembles $\{\bar{n} : n \in \xi\}$ ($\xi \in \mathfrak{P}(\mathbf{N})$).

4. Soit $\mathscr{L}$ un langage dénombrable égalitaire à k types de variables tel que $C_{\mathscr{L}}^{(1)} \supset \mathbf{N}$ (autrement dit les entiers naturels sont des symboles de constante de type 1 de $\mathscr{L}$). Une réalisation égalitaire de $\mathscr{L}$, ayant pour ensembles de base $U_1, \dots, U_k$, est appelée ω-réalisation si et seulement si $U_1 = \mathbf{N}$ et $\bar{n} = n$ pour chaque $n \in \mathbf{N}$, $\bar{n}$ étant la valeur prise par n dans la réalisation considérée. Soit $\mathscr{A}$ un ensemble de formules closes de $\mathscr{L}$ qui contient la formule $n \neq n'$ pour tout couple (n, n') d'entiers naturels distincts.

a) Montrer que l'ensemble des formules satisfaites par tous les ω-modèles de $\mathscr{A}$ est le plus petit ensemble $\mathscr{A}^\omega$ de formules de $\mathscr{L}$ tel que : $\mathscr{A} \subset \mathscr{A}^\omega$; pour toute formule close F, et toute formule Gx de $\mathscr{L}$, si $\mathscr{A}^\omega \vdash F$ alors $F \in \mathscr{A}^\omega$; si, pour tout entier n, $\mathscr{A}^\omega \vdash Gn$, alors $\bigwedge x Gx \in \mathscr{A}^\omega$.

b) En utilisant le théorème 3, montrer que si $X \subset \mathbf{N}$ est définissable (chap. précédent) dans tous les ω-modèles de $\mathscr{A}$ il existe deux formules F et Gx, x étant de type 1, telles que, pour tout $p \in \mathbf{N}$

$$p \in X \Leftrightarrow \mathscr{A}^\omega \cup \{F\} \vdash Gp, \qquad p \notin X \leftrightarrow \mathscr{A}^\omega \cup \{F\} \vdash \neg Gp.$$

c) Montrer que a) serait faux sans la restriction à des langages dénombrables.

Solution.

a) Une réalisation égalitaire de $\mathscr{L}$ est une ω-réalisation si et seulement si elle satisfait la formule infinie $\bigwedge x \bigvee_n x = n$. On applique le théorème 4.

b) Remarquons d'abord que, dans une ω-réalisation de $\mathscr{L}$, un sous-ensemble X de $\mathbf{N}$ est définissable si et seulement si il est définissable sur $\mathbf{N}$ (en effet, $\mathbf{N}$ est l'ensemble de base de type 1 de la réalisation en question).

Pour toute formule $A(x, x_1, \dots, x_n)$ et tout entier p, posons

$$A_p(x_1, \dots, x_n) = A(p, x_1, \dots, x_n) \qquad \text{si} \quad p \in X$$

et

$$A_p(x_1, \dots, x_n) = \neg A(p, x_1, \dots, x_n) \quad \text{si} \quad p \notin X.$$

Comme X est définissable dans tous les ω-modèles de $\mathscr{A}$, chacun d'eux satisfait une des formules infinies

$$\vee x_1 \dots \vee x_n \bigwedge\!\!\!\bigwedge_p A_p(x_1, \dots, x_n)$$

pour une certaine formule $A(x, x_1, \dots, x_n)$ de $\mathscr{L}$. Donc tout modèle de $\mathscr{A}$ satisfait soit une de ces formules soit $\vee x \bigwedge\!\!\!\bigwedge_p (x \neq p)$, x étant de type 1, et tout modèle de $\mathscr{A}^\omega$ satisfait une des formules infinies, soit

$$\vee x_1 \dots \vee x_n \bigwedge\!\!\!\bigwedge_p A_p(x_1, \dots, x_n) .$$

En appliquant le corollaire du Théorème 3 on voit qu'il existe une formule $B(x_1, \dots, x_n)$ telle que : $\mathscr{A}^\omega \cup \{ \vee x_1 \dots \vee x_n\, B(x_1, \dots, x_n) \}$ est consistant et

$$\mathscr{A}^\omega \vdash \wedge x_1 \dots \wedge x_n [B(x_1, \dots, x_n) \to A_p(x_1, \dots, x_n)]$$

pour chaque entier p. En prenant

$$\vee x_1 \dots \vee x_n\, B(x_1, \dots, x_n) \qquad \text{pour } F$$

et

$$\vee x_1 \dots \vee x_n [B(x_1, \dots, x_n) \wedge A(x, x_1, \dots, x_n)] \qquad \text{pour } Gx$$

on obtient le résultat cherché. (Ce résultat peut aussi être démontré par la méthode du Théorème 5, Chap. 6.)

c) La partie *b*) de l'exercice précédent donne la solution parce que $J = \wedge x \bigvee\!\!\!\bigvee_n (x = n)$, c'est-à-dire que l'ensemble $\mathscr{A}$ qui y est défini n'a pas de ω-modèle, bien que $\mathscr{A}^\omega$ soit consistant.

5. *a*) Définir les classes suivantes de structures en utilisant des formules infinies : (i) Corps ordonnés archimédiens, (ii) Groupes engendrés par les p générateurs $a_1, a_2, \dots, a_p$, (iii) Ensembles des types $\leqslant \tau$ héréditairement finis.

b) Montrer que chacune des classes (i)-(iii) définies dans *a*) est la classe des modèles d'une seule formule du second ordre, et qu'aucune d'entre elles n'est la classe des modèles d'un ensemble de formules finies du premier ordre.

Solution.

a) (i) On considère le langage des corps ordonnés, les axiomes pour ces corps, et on ajoute la formule $\wedge x \bigvee\!\!\!\bigvee_n (x < \sigma_n)$, où σ_1 est 1 et σ_{n+1} désigne le terme $(\sigma_n + 1)$. (ii) On considère le langage de groupe,

les axiomes de groupe, et la formule $\bigwedge x \bigvee\!\!\bigvee_n (x = s_n)$, où s_n est une énumération de tous les termes

$$a_1^{\rho_{11}} \dots a_p^{\rho_{1p}} \dots a_1^{\rho_{n1}} \dots a_p^{\rho_{np}},$$

et

$$\rho_{ij}\,(1 \leqslant i \leqslant n, 1 \leqslant j \leqslant p) = 1 \text{ ou } -1 \text{ ou } = 0\,.$$

(iii) On considère le langage $\mathscr{L}$ dont le seul symbole relationnel est $=$, et on construit $\mathscr{L}^\tau$ comme dans le Chap. 5. Les axiomes sont ceux de la théorie des types et, en plus, pour tout $\sigma \leqslant [\tau]$, où $\sigma = (\sigma_1, \dots, \sigma_p)$, $\bigwedge x^\sigma \bigvee\!\!\bigvee_n E_n\, x$, où $E_n\, x$ est la formule

$$\bigwedge x_1^{\sigma_1} \dots \bigwedge x_{n+1}^{\sigma_1} \dots \bigwedge x_1^{\sigma_p} \dots \bigwedge x_{n+1}^{\sigma_p}([(x_1^{\sigma_1}, \dots, x_1^{\sigma_p})\, \varepsilon_\sigma\, x \wedge \cdots$$
$$\wedge\ (x_{n+1}^{\sigma_1}, \dots, x_{n+1}^{\sigma_p})\, \varepsilon_\sigma\, x] \to [\cdots \vee (x_i^{\sigma_1} = x_j^{\sigma_1} \wedge \cdots \wedge x_i^{\sigma_p} = x_j^{\sigma_p}) \vee \cdots])$$
$$(1 \leqslant i < j \leqslant n+1)\,.$$

b) Il est évident (Chap. 3, exercice 1) qu'aucune de ces classes n'est la classe des modèles d'un ensemble de formules du premier ordre ; (i) voir chap. 3, exercice 7, (ii) on ajoute une nouvelle constante a et les axiomes $s_1 \neq a$, $s_2 \neq a, \dots$, (iii) on ajoute une constante $a^{(0)}$ de type (0), les constantes $c_1, c_2, \dots$ du type 0, et les axiomes $c_n\ \varepsilon_{(0)}\, a^{(0)}$ pour $n = 1, 2, \dots$ et $c_n \neq c_m$ pour tout couple (n, m) d'entiers distincts. Par contre, toute formule infinie de *a*) équivaut à une seule formule de second ordre. On considère les deux cas : la variable X varie : α) sur la famille de tous les sous-ensembles de l'ensemble de base de la réalisation considérée, β) sur la famille de tous ses sous-ensembles finis (voir chap. 5, Ex 6 *b*)).
(i) On écrit A pour

$$\bigwedge X\{[z e X \wedge \bigwedge y(y + 1\, e X \to y\, e X)] \to 1\, e X\}$$

et B pour

$$\bigvee X[1\, e X \wedge \bigwedge y(y \neq z \wedge y\, e X \to y + 1\, e X)]\,.$$

Dans les deux cas on a :

$$\bigvee\!\!\bigvee_n (z = \sigma_n) \to A\,.$$

Dans le cas α) on a aussi

$$A \to \bigvee\!\!\bigvee_n (z = \sigma_n)\,,$$

dans le cas β) on a

$$B \to \bigvee\!\!\bigvee_n (z = \sigma_n)\,.$$

Par conséquent, dans les deux cas, on a

$$\bigvee\!\!\!\bigvee_n (z = \sigma_n) \leftrightarrow (A \wedge B),$$

$\wedge z B$ étant vraie dans le cas α). Puisque $\bigvee\!\!\!\bigvee_n (x < \sigma_n)$ équivaut à

$$\vee z\Big[x < z \wedge \bigvee\!\!\!\bigvee_n (z = \sigma_n)\Big],$$

on a

$$\bigvee\!\!\!\bigvee_n (x < \sigma_n) \leftrightarrow \vee z(x < z \wedge A \wedge B)$$

dans les deux cas.

(ii) On ne considère que le cas (α) ; la modification requise dans le cas (β) est analogue à (i) :

$$\bigvee\!\!\!\bigvee_n (x = s_n) \leftrightarrow \wedge X[(xeX \wedge \wedge y[(ya_1\, eX \vee ya_1^{-1}\, eX \vee \cdots \vee ya_p\, eX \vee ya_p^{-1}\, eX) \rightarrow yeX]) \rightarrow 1\, eX].$$

(iii) On écrit $z = y \cup (z_1, ..., z_p)$, z_i étant un terme de type σ_i, pour $1 \leqslant i \leqslant p$, pour

$$\wedge x_1^{\sigma_1} \ldots \wedge x_p^{\sigma_p}((x_1, ..., x_p)\, \varepsilon_\sigma\, z \leftrightarrow \leftrightarrow [(x_1, ..., x_p)\, \varepsilon_\sigma\, y \vee (x_1 = z_1 \wedge \cdots \wedge x_p = z_p)]).$$

Alors, dans le cas α), si $x, y, z, z_1, ..., z_p$ sont des variables de type $\sigma, \sigma, \sigma, \sigma_1, ..., \sigma_p$ respectivement, $\bigvee\!\!\!\bigvee_n E_n\, x$ équivaut à

$$\wedge X \{ \wedge y \wedge z \wedge z_1 \ldots \wedge z_p[[yeX \wedge y = z \cup (z_1, ..., z_p)] \rightarrow \rightarrow (z_1\, eX \wedge \cdots \wedge z_p\, eX \wedge zeX)] \rightarrow [xeX \rightarrow \phi eX] \}.$$

APPENDICE I

LA MÉTHODE AXIOMATIQUE

Le caractère général de cette méthode est habituellement décrit comme suit. A la place d'affirmations concernant certaines propriétés abstraites d'objets et de concepts de nature variée (espace, point matériel, probabilité, etc.), on considère des affirmations de la forme suivante : pour toute collection d'objets (dont la nature n'est pas autrement spécifiée) et pour tout système de relations entre ces objets, si ces relations vérifient certaines conditions purement logiques ([1]) données (qu'on appelle les axiomes), alors elles vérifient aussi certaines autres conditions purement logiques (qu'on appelle les théorèmes de la théorie axiomatique correspondante). Dans diverses parties des mathématiques axiomatiques ordinaires, un petit nombre de systèmes axiomatiques particuliers ont été isolés et étudiés ; grâce à ce procédé, une bonne partie des mathématiques a été édifiée d'une façon systématique et compréhensible. On ne s'est pas intéressé aux systèmes axiomatiques *quelconques*, ni même à des *classes* générales de systèmes axiomatiques. Aussi l'expérience tirée des mathématiques « ordinaires » ne fournit-elle aucune raison de supposer que, pour des classes générales de systèmes axiomatiques, on puisse obtenir des résultats utiles contribuant à l'emploi efficace de la méthode axiomatique.

Nous voudrions présenter ici certaines applications d'une étude portant sur des classes générales de systèmes axiomatiques. La classe d'axiomes que nous étudierons principalement — mais non exclusivement — est celle de la *logique des prédicats du premier ordre*, qui est définie de façon précise dans les chapitres 1 et 2. En gros, cette classe est caractérisée par le fait que les formules considérées expriment certaines propriétés de relations et d'opérations portant sur un domaine E, et que dans la définition de ces propriétés interviennent seulement des quantifications portant sur les éléments de E, et non pas sur les sous-ensembles de E, etc. Exemples : le fait qu'une relation est une relation d'ordre s'exprime par une formule du premier ordre, mais non pas le fait que c'est une relation de bon-ordre. Ou encore, la propriété d'être un groupe (c'est-à-dire, pour une relation $a \circ b = c$, de satisfaire les axiomes de groupe) est du premier ordre, ainsi que celle d'être un groupe commutatif. La propriété d'être un groupe ordonnable ne se *définit* pas en termes

(1) Logique est pris ici dans le sens que lui donne Bourbaki, Chap. XXII, p. 73.

du premier ordre, puisqu'elle s'exprime par : « il existe une relation d'ordre sur E compatible avec l'opération de groupe, c'est-à-dire un *sous-ensemble* de E^2 tel que... » ; mais cette propriété est équivalente à un certain ensemble *infini* de conditions du premier ordre. Enfin la propriété d'être un groupe à nombre fini de générateurs, et celle d'être un groupe dénombrable, ne sont pas équivalentes à des ensembles, même infinis, de conditions du premier ordre.

Ainsi la classe des systèmes axiomatiques pour laquelle nous obtenons ces résultats généraux ne contient pas toutes les mathématiques usuelles, à cause de la restriction sur les quantifications d'ordre supérieur. En compensation, nous employons des systèmes infinis d'axiomes, c'est-à-dire que nous considérons des structures vérifiant un ensemble infini de conditions, et pouvons ainsi manier toute une classe de problèmes qui sont *formulés* en termes d'ordre supérieur, mais sont *réductibles* a des problèmes portant sur des ensembles infinis de conditions du premier ordre. Les exemples sont donnés dans les chapitres 1 et 3, principalement en exercices. Les résultats généraux les plus utiles sont les suivants, tous reliés entre eux : 1° le théorème de finitude : si une formule A du premier ordre est satisfaite dans toutes les structures qui satisfont une classe $\mathscr{A}$ de formules du premier ordre, alors il existe un sous-ensemble fini $\mathscr{A}_1$ de $\mathscr{A}$ qui implique A ; 2° la méthode des constantes (exercice 2 du chapitre 3) qui généralise le principe — bien connu en algèbre — d'introduction d'éléments transcendants (par exemple, on déduit une structure contenant un élément ξ telle que $p_n(\xi) \neq 0$ pour tout n à partir d'une structure qui, pour tout n, contient un élément ξ_n satisfaisant $p_i(\xi_n) \neq 0$ pour tout $i \leqslant n$). 3° le théorème de plongement qui fournit une condition nécessaire et suffisante pour qu'une structure soit plongeable dans une autre qui satisfasse une classe donnée $\mathscr{A}$ d'axiomes. (Les affirmations au sujet des groupes dans le précédent paragraphe sont des corollaires immédiats des 1° et 3°). Ces théorèmes permettent de simplifier plusieurs résultats connus qui consistent à passer des sous-systèmes finis au système entier, ou à obtenir des conditions de plongement (équationnelles) du premier ordre. Mais le principal intérêt de ces théorèmes, c'est peut-être d'éclaircir le caractère général d'un problème, en montrant ce qui est général et ce qui est particulier. Ainsi à première vue, il peut paraître remarquable qu'il existe une condition algébrique, c'est-à-dire du premier ordre, qui est nécessaire et suffisante pour qu'un corps soit ordonnable

$$(x_1^2 + \cdots + x_n^2 + 1 \neq 0, \quad \text{pour } n = 1, 2, ...) ;$$

or, en tant que résultat général, c'est là une conséquence immédiate du 3° ci-dessus ; et c'est seulement sur des points de détail que les conditions trouvées demandent un examen spécial, par exemple pour montrer que cet ensemble de conditions ne peut pas être remplacé par un ensemble fini. Notons en passant qu'il existe une intéressante théorie qui relie les propriétés algébriques usuelles de certaines classes de structures à la forme *syntaxique* des axiomes définissant ces classes. Ainsi les axiomes de groupe sont purement équationnels ; les

axiomes de corps contiennent des combinaisons propositionnelles d'équations (équations conditionnelles) : $x = 0 \vee xx^{-1} = e$; les axiomes de corps algébriquement clos et ceux de corps réels fermés sont tous de la forme : quantificateurs universels suivis de quantificateurs existentiels suivis d'une combinaison d'équations. Cette théorie permet de répondre à des questions comme : Pourquoi le fait qu'un corps est ordonnable peut-il être exprimé par des ensembles d'inéquations et non pas par des ensembles d'équations ? Réponse : si un ensemble d'équations est satisfait dans une certaine structure, alors il est satisfait dans toute image homomorphe d'une sous-structure quelconque de cette structure ; par conséquent, si un ensemble d'équations est satisfait dans le corps des rationnels, il est aussi satisfait dans le corps des entiers modulo 2 ; mais le corps des rationnels est ordonnable alors que celui des entiers modulo 2 ne l'est pas. Pour des développements récents de cette théorie, cf. l'ouvrage de A. Robinson, *Introduction to model theory and to the metamathematics of algebra*, Amsterdam (1963) North Holland Publishing Co. (Le chapitre 6 du présent ouvrage expose les méthodes de cette théorie.)

Le chapitre 4 illustre un emploi plus spécifique de la notion de formule du premier ordre, emploi qui permet d'extraire toute la « force » de certaines constructions particulières. Ainsi la théorie du résultant en algèbre permet de trouver une condition équationnelle par rapport aux coefficients de deux polynômes qui est nécessaire et suffisante pour que ces polynômes aient une racine commune. Mais la même construction fournit beaucoup plus, à savoir un ensemble de conditions analogues pour une formule du premier ordre quelconque dans la théorie des corps algébriquement fermés ! Semblable, mais plus intéressant, est le cas des corps réels fermés. Sturm a montré, il y a longtemps, qu'un polynôme s'annule sur le segment fermé (a, b) si et seulement si une certaine inégalité polynomiale est satisfaite (les termes de cette inégalité étant obtenus rationnellement à partir de a, b, et des coefficients du polynôme donné). Artin et Schreier ont isolés les axiomes sur lesquels repose cette équivalence, à savoir ceux des corps réels fermés. Une fois qu'on possède la notion de formule du premier ordre, il est naturel de chercher à étendre cette méthode afin d'englober *toutes* les formules du premier ordre dans la théorie des corps. Ce problème a été mentionné par Herbrand, et complètement traité par Tarski, qui a montré que *toute* formule du premier ordre de la théorie considérée est équivalente à une combinaison booléenne d'égalités et d'inégalités polynomiales. En particulier, lorsqu'une telle formule est sans variables libres, ou bien elle est vraie dans tous les corps réels fermés, ou bien elle est fausse dans tous. En d'autres termes, bien que les corps réels fermés ne soient évidemment pas tous isomorphes, ils sont néanmoins équivalents par rapport aux formules du premier ordre construites à partir d'égalités et d'inégalités polynomiales. On en déduit une démonstration presque immédiate du théorème d'Artin sur la représentation des formes définies positives comme sommes de carrés de formes rationnelles, démonstration qui est donnée en exercice dans le chapitre 4.

Les ensembles $\mathscr{A}$ d'axiomes dont tous les modèles sont équivalents vis-à-vis des formules du premier ordre (exprimables dans les notations de $\mathscr{A}$) sont dits *saturés* ou *complets*. Une remarquable théorie des modèles de ces ensembles $\mathscr{A}$ a été récemment édifiée par Morley (*Trans. Ann. Math. Soc.*, **114** (1965), 514-438), théorie qui est étroitement parallèle à la théorie de Cantor des sous-ensembles fermés de la droite. Les ensembles fermés qui viennent tout d'abord à l'esprit sont très particuliers ; s'ils ne sont pas parfaits au départ, leur premier ou second dérivé est parfait (éventuellement vide), bien que, pour chaque ordinal dénombrable α, il existe un ensemble fermé dont le α-ème dérivé n'est pas parfait. De même, pour les quelques ensembles complets $\mathscr{A}$ qui se sont présentés dans d'autres branches des mathématiques, les ordinaux qui leur correspondent dans la théorie de Morley sont finis, bien que pour chaque ordinal α dénombrable, il existe un ensemble complet (et dénombrable) auquel correspond cet α.

Le théorème de finitude (p. 150) entraîne que tout système d'axiomes du premier ordre possédant un modèle infini possède aussi nécessairement des modèles infinis de différentes cardinalités (et par conséquent non isomorphes). Historiquement, c'est pour caractériser de façon unique certaines structures infinies que furent introduits les premiers systèmes d'axiomes — et les plus connus —, par exemple les axiomes de Peano pour l'arithmétique et ceux de Dedekind pour le continu. En regardant de plus près ces systèmes d'axiomes, on s'aperçoit que leur interprétation usuelle ne prend pas en considération la totalité des modèles généraux, mais seulement certains d'entre eux ; autrement dit, ce n'est pas seulement la signification des symboles logiques qui est imposée, mais aussi celle de certains autres symboles. En particulier, dans les systèmes d'axiomes classiques apparaissent certaines « variables d'ensembles », et les modèles considérés sont ceux où ces variables décrivent l'ensemble de *tous* les sous-ensembles (de l'ensemble appelé E à la p. 149). Les langages qui contiennent de telles variables d'ensembles sont dits d'*ordre supérieur*, et les modèles de l'espèce restreinte qu'on vient de décrire sont dits *principaux*. Les systèmes d'axiomes de Peano et de Dedekind sont du second ordre. On trouvera dans le chapitre 7 quelques résultats isolés, par exemple la réduction de la validité d'ordre n (pour n fini > 2) à la validité du second ordre, mais la plupart des résultats généraux concernant les systèmes du premier ordre ne se laissent pas étendre au cas supérieur. On définit une classe intermédiaire de modèles, celle des « ω-modèles », en imposant à l'un des symboles de relation monadique d'être réalisé par l'ensemble des nombres naturels, et à l'un des symboles de relation dyadique d'être réalisé par la relation de successeur. On rencontre constamment de telles classes de structures dans les mathématiques courantes, par exemple les espaces vectoriels sur le corps des rationnels ; par contre, la classe des espaces vectoriels sur un corps quelconque (non fixé) n'est autre que la classe de tous les modèles (sans restriction) d'un certain système d'axiomes de premier ordre. Dans le chapitre 7, certains résultats concernant les modèles généraux sont étendus aux ω-modèles, et on trouvera beaucoup plus sur ce

sujet dans les références qui accompagnent le résumé du chapitre 6 ; mais contrairement aux cas des modèles généraux, il est souvent essentiel que les axiomes soient en infinité dénombrable, du moins lorsqu'on se borne aux formules finies.

Les résultats « négatifs » de non-catégoricité (relatifs aux systèmes d'axiomes du premier ordre) ont comme côté « positif » l'existence de modèles non principaux (dits aussi : non-standards, exercice 2 du chapitre 3). Tout récemment, on a utilisé ces modèles pour édifier l'Analyse non-standard. Elle diffère essentiellement des autres tentatives d'Analyse sur un corps non archimédien K en ce qu'elle fait intervenir l'ensemble des « entiers de K » (qui satisfait les axiomes arithmétiques qu'on s'est donné). L'existence de modèles non principaux implique l'existence de corps non archimédiens admettant de tels « entiers » (non archimédiens) et non pas seulement des « réels » non archimédiens (par exemple, dans une série de Taylor $\Sigma a_n x^n$, la variable n varie sur tous les entiers de K et non pas seulement sur les entiers standards). On trouve un exposé de cette véritable Analyse infinitésimale dans l'ouvrage de A. Robinson, *Non-standard analysis*, Amsterdam (1966), North Holland Publishing Co.

Jusqu'ici, on a mis en évidence les applications au sens strict du mot : les techniques indiquées dans le texte permettaient de répondre à des questions explicitement formulées dans le langage mathématique ordinaire. Il reste à examiner ce qui constitue, à long terme, le rôle le plus fructueux des notions nouvelles, à savoir la possibilité de formuler certaines questions que nous avons dans l'esprit sans que nous soyons capables de les exprimer de façon précise dans le langage mathématique ordinaire (et il resterait encore, bien entendu, les applications éventuelles à certaines branches inhabituelles des mathématiques). Dans cet ordre d'idées, l'exemple le plus frappant est peut-être constitué par la théorie des ensembles uniformément définissables, indiquée dans le chapitre 6, qui peut être illustrée par les questions élémentaires suivantes : considérons les corps commutatifs de caractéristique nulle, ils contiennent tous un sous-corps isomorphe au corps des rationnels. Posons-nous les questions suivantes : 1° (resp. : 2°) quelles sont les formules du premier ordre $A(x)$ qui définissent le même ensemble de rationnels dans chacun des corps considérés, c'est-à-dire sont satisfaites dans chacun de ces corps par les mêmes rationnels (resp. : et seulement par des rationnels) ? 3° quels sont les ensembles de rationnels qui peuvent être ainsi définis ? 4° quels sont les ensembles de rationnels qui, dans chaque corps commutatif de caractéristique nulle, peuvent être définis par une formule du premier ordre dépendant éventuellement du corps considéré ? Les solutions complètes de ces problèmes s'obtiennent comme corollaires de théorèmes tout à fait généraux relatifs à des systèmes d'axiomes quelconques. Le 3° et le 4° sont équivalents, ce qui fournit une nouvelle et puissante condition d'uniformité ; la réponse au 2° est constituée seulement par les formules définissant des ensembles finis : autrement dit, il faut abandonner l'espoir de distinguer les rationnels par une condition du premier ordre qui soit la même dans tous les corps — et, en fait, il existe même un corps

commutatif de caractéristique nulle dans lequel les rationnels ne peuvent pas être distingués par une condition du premier ordre (un algébriste dirait : ne peuvent pas être algébriquement caractérisés). Il suffit de réfléchir un instant pour voir que ces questions ne sont intéressantes que si l'on s'autorise à considérer une formule A arbitraire du premier ordre, et non pas seulement des équations ou des combinaisons propositionnelles d'équations. C'est évidemment là une raison supplémentaire pour que les questions ci-dessus n'aient jamais été traitées dans la littérature mathématique « ordinaire ».

Ce travail sur les ensembles définissables dans les modèles généraux s'étend aussi aux ω-modèles décrits ci-dessus. Il fournit une application de la théorie des modèles à deux autres branches de la logique, non traitées dans ce livre : la théorie des ensembles récursifs et celle des ensembles hyperarithmétiques. Cette application est fondée sur les faits suivants : d'une part les éléments de base en théorie de la récursivité sont 1° les ensembles finis (de nombres naturels), 2° les ensembles récursifs ; d'autre part, les ensembles uniformément définissables dans les systèmes axiomatiques usuels pour l'arithmétique ne sont autres que les ensembles finis si la définissabilité est prise au sens 2° du précédent paragraphe, les ensembles récursifs si elle est prise au sens 1°. On peut alors généraliser la théorie de la récursivité dans deux directions : en remplaçant les systèmes d'axiomes usuels pour l'arithmétique par d'autres systèmes, et en remplaçant la classe des modèles généraux par d'autres classes de modèles.

APPENDICE II

FONDEMENTS DES MATHÉMATIQUES

Introduction.

La théorie des fondements décrit et analyse les mathématiques dites « intuitives », c'est-à-dire telles qu'elles se présentent à l'esprit des mathématiciens de métier.

La partie descriptive formule la pratique mathématique dans un langage formel (par exemple le langage ensembliste). Ceci épure et précise la pratique parce que, contrairement aux langages courants, les langages formels ont un vocabulaire très réduit et une grammaire parfaitement exacte. La partie descriptive n'est évidemment qu'une partie auxiliaire des fondements : comme toute description des connaissances intuitives, elle fait intervenir comme essentielle l'idée ou la conception qu'on a des choses décrites ; en particulier, le langage formel ne se rapproche point du langage de la pratique sur le plan syntaxique (heureusement), mais il exprime correctement les énoncés formulés par elle. On note aussi que la précision du langage formel, bien que fort utile pour le développement technique, n'aide guère à résoudre des difficultés dues à une conception défectueuse (au contraire, c'est la réflexion sur la conception intuitive qui conduit à un bon langage). Par exemple, dans les « crises » bien connues, voir A, § 1 ci-dessous, les contradictions découlaient de principes (axiomes, règles d'inférences) tout à fait explicites, ce qui montre qu'il ne s'agissait point d'un manque de précision formelle ; parmi des principes formellement précis, on ne savait pas distinguer les bons des mauvais.

Les fondements proprement dits s'occupent de ce genre de question, ce qui peut réclamer des considérations nettement différentes de celles de la pratique mathématique. En particulier, les fondements cherchent (un cadre qui permette la formulation) de bonnes raisons *pour* les principes de base que la pratique accepte, tandis que celle-ci ne s'occupe que des démonstrations *à partir de* ces principes. Les méthodes utilisées dans une telle analyse *approfondie* de la pratique conduisent souvent à une *extension* de sa compréhension théorique. Un cas particulièrement important est la recherche de nouveaux axiomes de base, ce qui n'est rien d'autre que la continuation de la recherche qui a fourni les axiomes de base courants.

D'après ce qu'on vient de dire les fondements doivent dépasser la pratique. Découvrir ces nouvelles notions et ces nouvelles méthodes peut avoir une saveur philosophique incontestable. 1° Si l'on pense que ce qui est significatif dans les mathématiques intuitives concerne certains objets (abstraits) on aboutira à une théorie « réaliste » de ces objets de base : les fondements ainsi obtenus analyseront les significations des énoncés intuitifs en termes de cette théorie et dériveront les règles du raisonnement des lois auxquelles obéissent les objets de base. On peut comparer des fondements réalistes à une physique générale qui interprète l'expérience physique ordinaire en terme de composants fondamentaux du monde matériel (les particules élémentaires dans la physique générale courante). 2° Si, par contre, on pense que la preuve ou, plus spécialement, les espèces de preuves constituent l'essentiel des mathématiques intuitives on essaiera de formuler les fondements dans des termes « idéalistes » qui se réfèrent à l'activité mathématique elle-même. On trouve un exemple du 1° dans la partie A ci-dessous sur les *fondements sémantiques ensemblistes* [ici les significations des formules sont les réalisations des chapitres 2, 7] ; et un exemple du 2° dans B, qui esquisse les *fondements syntaxiques combinatoires* (prenant, d'ailleurs, l'activité mathématique dans un sens plutôt étroit). On mentionnera des inconvénients de ces deux théories des fondements dans B, § 4 *a*).

Signalons ici deux difficultés particulièrement notables dans les fondements (mais aussi présentes dans toute tentative de compréhension théorique). Premièrement, pour décider entre deux conceptions rivales il faut en sortir : si, consciemment ou non, on accepte l'une on risque de ne pas prendre au sérieux l'autre ! Aux yeux du réaliste en question, l'autre néglige l'essentiel, à savoir les objets de base, et se perd dans des distinctions mineures (qui sont peut-être analogues à la distinction entre les observations à l'œil nu et celles à l'aide du microscope, distinction à laquelle on n'attribue aucune signification physique). En revanche, l'idéaliste trouve bizarre l'idée de dériver le raisonnement intuitif des lois hypothétiques sur ces objets abstraits qu'il considère comme douteux ou, tout au moins, comme peu essentiels aux mathématiques. Deuxièmement, si les conceptions considérées sont vieilles et donc viables, elles sont forcément en accord avec toutes les mathématiques élémentaires ; par conséquent, la décision entre les conceptions peut réclamer un développement des mathématiques intuitives (ce qui correspond à la découverte d'un experimentum crucis en physique théorique). Il va de soi qu'un appareil déjà fort compliqué peut être nécessaire à la formulation même d'une conception : y parvenir est une des tâches principales de la logique mathématique.

Quant à l'utilité des fondements pour les mathématiques intuitives, elle est tout à fait parallèle à celle d'autres analyses théoriques. On trouvera dans l'appendice I quelques applications de l'analyse sémantique. Et on a appliqué les méthodes de l'analyse syntaxique aux machines à calculer : ce qui n'a rien d'étonnant, puisqu'une des idées qui se trouvent à son origine c'est que le

raisonnement mathématique est mécanisable. En bref, l'utilité des fondements est, en principe, hors de question.

Dans des cas particuliers nous avons la situation suivante. Si une question, disons en théorie des nombres, est formellement indécidée par les axiomes de base de la pratique, sa solution peut réclamer l'aide de la théorie des fondements : d'abord pour établir cette indécidabilité et ensuite pour trouver de nouveaux axiomes (et ces possibilités sont réalisées dans A, § 3). Mais à l'heure actuelle la situation est confuse en Arithmétique ou Analyse : d'une part on ignore des questions qui sont effectivement étudiées dans la pratique mais indépendantes des axiomes courants, voir B, §1*c* ; d'autre part pour en trouver on ne peut faire confiance aux mathématiciens qui ne connaissent pas les méthodes de la théorie des fondements (de même qu'on n'a trouvé en Arithmétique que peu d'aspects relevant de la théorie des groupes tant qu'on n'a pas d'abord maîtrisé cette théorie).

Fondement et erreur. Un problème philosophique classique est de se demander comment éliminer éventuellement l'erreur de l'expérience naïve. Les fondements décrits ici ne fournissent que peu d'éléments pour le résoudre (et, en particulier, la formalisation, d'elle-même, n'en fournit aucun). On ne peut exclure la possibilité qu'il y ait des erreurs de base à éliminer ; mais les deux exemples, souvent cités, de convictions naïves trompeuses, ne sont pas concluants, à savoir les paradoxes de la théorie des ensembles (A, § 2) et l'existence en arithmétique de propositions formellement indécidables (A, § 3). En fait, les objections que firent les mathématiciens à l'introduction de la notion d'ensemble (alors appelée « classe ») sont légendaires, ainsi que leurs efforts pour montrer que le raisonnement mathématique (même en géométrie élémentaire !) n'est pas mécanisable. Au plus, l'attitude naïve a été hyper-conservatrice.

Une doctrine anti-philosophique (positiviste). Cette doctrine courante voudrait confiner les fondements à leur partie descriptive et, en particulier, supprimer les questions traditionnelles de fondements plutôt que les résoudre parce que, d'après cette doctrine, elles manquent de précision. On a noté les inconvénients fondamentaux d'une telle restriction au début de la présente introduction et on les considérera de près par rapport aux fondements sémantiques dans A, § 4*c*) et par rapport aux fondements combinatoires dans B, § 4. Mais, il convient de signaler ici quelques considérations générales au sujet de la doctrine en question.

La précision qu'elle sous-entend réclame une formulation en termes dits « positivistes » ou « opérationnels » ce qui revient à « formels » en mathématiques. Cette exigence, à son tour, repose sur la découverte [A, § 4a)] que le raisonnement logique élémentaire [c'est-à-dire, du premier ordre] est sinon formel (mécanique), du moins formalisable (mécanisable). Avant cette découverte, la philosophie positiviste n'avait aucun point d'appui dans le raisonnement mathématique.

On note d'abord que l'énoncé même de cette découverte fait intervenir la notion intuitive de conséquence logique : en l'acceptant on *montre* son équivalence avec une certaine relation formelle. Cela n'élimine point la notion intuitive, mais, au contraire, en établit une propriété fondamentale, à savoir l'existence d'un critère formel. Le positivisme va plus loin : ayant formulé (correctement) le critère de précision formelle, il conclut (à tort) que ce critère caractérise les limites effectives de la pensée mathématique. Les progrès des fondements et, d'ailleurs, des mathématiques intuitives montrent le contraire. Les bons mathématiciens savent souvent juger (collectivement), avec certitude de la valeur d'une réponse aux questions qui ne sont pas formulées avec précision formelle : par exemple si oui ou non un axiome est valide pour une notion intuitive (voir A, § 2*c*), B, § 2*c*)), une définition bonne (par exemple de la longueur d'une courbe). On dit parfois que ce genre de question n'appartient pas aux mathématiques ; opinion bizarre car, d'une part, on ne dit pas à quel domaine elle appartiendrait et de l'autre, ce sont les mathématiciens qui s'en occupent. Puisque ils sont d'accord entre eux (et c'est là une constatation de fait que les positivistes passent sous silence), on ne voit pas pourquoi on qualifierait de subjective ce genre de question. Bref, les faits empiriques mettent en question la nécessité et donc, à la longue, la fécondité de la restriction positiviste et non point le bon sens des problèmes de fondements, tout au moins, de la plupart d'entre eux. (Comme dans toute théorie, seule la recherche peut décider exactement jusqu'où il est possible d'aller ; souvent les cas limites attirent le plus l'attention.)

Le positivisme semble avoir une certaine valeur pragmatique. Quant à la recherche on a vu dans l'appendice I quelques conséquences utiles de la réduction d'une notion abstraite à une notion formelle, à savoir de « validité dans toute structure mathématique » à « conséquence formelle » (dans le cas des énoncés élémentaires [du premier ordre]). Aussi a-t-on noté ci-dessus que la théorie des fondements peut être inutile dans certains domaines de la pratique, au moins à un moment donné. En ce qui concerne l'enseignement on trouve que la théorie des fondements attire, principalement, ou bien ceux qui sont doués pour la philosophie ou bien ceux qui n'y comprennent rien (et de ce fait sont fascinés) : les uns ne seront pas séduits par l'erreur positiviste et les autres se consoleront avec une justification, même mauvaise, de leur état. Bien entendu, ils ne chercheront pas, disons, de nouveaux axiomes de base. Mais, n'importe comment, ils n'en trouveraient pas ; et, après tout, on peut s'occuper de problèmes d'ordre technique, c'est-à-dire de problèmes formulables dans le langage de la pratique. Ceci s'applique même en logique mathématique, par exemple dans les parties que ce livre expose : on perdra seulement ainsi l'élément le plus fécond de la logique mathématique, à savoir son côté spécifiquement logique ; en particulier, les conjectures directrices fournies par les diverses conceptions de la théorie des fondements.

A. FONDEMENTS SÉMANTIQUES ENSEMBLISTES

Les notions de base sont : les ensembles, la relation d'appartenance (entre ensembles) et les opérations « logiques » de réunion, complémentation et projection (d'ensembles).

Les fondements décrits dans cette section sont dits « sémantiques » parce qu'ils acceptent la terminologie ensembliste dans son sens propre et ne la considèrent pas comme une façon de parler appelant une analyse critique ; la signification pratique de cette distinction est particulièrement importante dans les § 2 et § 3 ci-dessous.

Avis au lecteur. — Les passages entre crochets réclament quelques connaissances techniques en logique mathématique (se rappeler l'avant-propos) ; les paragraphes mis en retrait concernent des questions fines d'ordre mathématique ou philosophique.

1. Comment analyse-t-on les mathématiques intuitives au moyen de ces notions de base, autrement dit : que signifie la « réduction » des mathématiques (intuitives) à la théorie des ensembles ?

Une *réalisation* [au sens des Chap. 2 et 7] est un ensemble, lui-même suite ordonnée des ensembles suivants : une collection d'individus, appelée parfois univers, puis des relations sur cet univers. La réduction ensembliste considère les structures mathématiques comme des réalisations. Ainsi l'arithmétique est l'univers constitué des entiers naturels, muni de la relation de successeur (sous-ensemble de $\mathbf{N} \times \mathbf{N}$) ; l'analyse est l'univers constitué des réels, muni des relations (sous-ensembles de $\mathbf{R}$ et $\mathbf{R} \times \mathbf{R}$) : « x est un rationnel » et la relation d'ordre (et ainsi d'autres structures définies en analyse, comme la géométrie : collection E_3 de points à 3 dimensions, munie d'une métrique).

A chaque structure mathématique S est associé un *langage* (« le langage de S »). Le langage n'exprime que des propriétés de la structure S, et non la nature des objets de son univers (le langage est purement logique [1]) : ainsi, si deux réalisations ayant même langage sont isomorphes, elles satisfont les mêmes assertions du langage. Un exemple d'un tel langage consiste en l'ensemble des formules construites à partir de symboles $R_1, ..., R_k$ pour les relations de S, de quantificateurs universel et existentiel, de la négation et de la conjonc-

---

(1) Voir note page 149.

tion [2]. [En d'autres termes : le calcul des prédicats du 1er ordre $\mathscr{L}_S$ dont les symboles de relation ont le même nombre d'arguments que les relations de S est purement logique, et bien entendu il en est de même du langage du Chap. 7, $\mathscr{L}^{\tau}_S$.]

NB. — Le mot « réalisation » est utilisé aussi dans l'expression « réalisation de la formule A dans la structure S », A étant une formule du langage de S comportant n variables libres $x_1, ..., x_n$: l'expression désigne la collection, notée aussi $\bar{A}$, des n-uplets $(\bar{x}_1, ..., \bar{x}_n)$ d'individus de S satisfaisant A.

La réduction ensembliste d'une structure S est exprimée par son axiomatisation *adéquate*, donnée d'un axiome $\mathscr{A}_S$ satisfaisant aux conditions suivantes :

$\mathscr{A}_S$ est purement logique.

S satisfait $\mathscr{A}_S$; par conséquent « il existe une réalisation qui satisfait $\mathscr{A}_S$ », ce qui est noté : $E^{\mathscr{A}_S}$.

Toutes les structures qui satisfont $\mathscr{A}_S$ sont isomorphes (donc isomorphes à S), propriété notée $U^{\mathscr{A}_S}$.

Toutes les propriétés intuitives de S s'expriment dans le langage de S ; propriété notée $X^{\mathscr{A}_S}$.

Toutes les assertions, formulées dans le langage de S, qui sont vraies pour S, sont conséquences logiques de $\mathscr{A}_S$; propriété notée $D^{\mathscr{A}_S}$.

Discussion :

(i) Dans $D^{\mathscr{A}_S}$ c'est la notion ordinaire en mathématiques de conséquence logique qui est utilisée [3]. A appartenant au langage de S, la différence entre « S satisfait A », et « A est conséquence logique de $\mathscr{A}_S$ » est évidemment que dans le dernier cas, A est vraie dans toute structure qui satisfait $\mathscr{A}_S$. Autrement dit, les propriétés explicitement postulées par $\mathscr{A}_S$ suffisent à elles seules pour conclure A. Par conséquent, si $U^{\mathscr{A}_S}$ est vrai, il y a équivalence entre : « S satisfait A », et : « A est conséquence de $\mathscr{A}_S$ ».

---

(2) Nous utilisons les notations de notre texte principal :
$\rightarrow$: implique (habituellement noté $\Rightarrow$)
$\neg$: non
$\wedge$: et (&)
$\vee$: ou
$\bigwedge$: pour tout ($\forall$)
$\bigvee$: il existe ($\exists$)

(3) Par exemple dans Bourbaki, les règles de déduction logique, qui sont énoncées dans le livre I chapitre I, ne sont plus jamais explicitement invoquées, au contraire des axiomes sur des structures particulières, comme les axiomes des groupes. Ceci montre bien que la notion de conséquence logique est supposée intuitivement comprise.

Mais notez qu'on peut également définir une « réduction » ensembliste de la notion intuitive de conséquence : la notion de *conséquence ensembliste.* Nous la formulons ici pour les langages dits du premier ordre, qui sont décrits dans l'App. I, p. 149, [ou dans le Chap. 2] :

On dit qu'une formule A d'un langage donné est conséquence ensembliste d'un ensemble $\mathscr{A}$ d'axiomes (du même langage) si elle est satisfaite par toute réalisation qui satisfait (toutes les formules de) $\mathscr{A}$.

Si A est conséquence de $\mathscr{A}$ au sens intuitif, A est aussi satisfaite par des « réalisations » en un sens plus large (cf. la notion étendue de réalisation, p. 162), qui satisfont $\mathscr{A}$. Par conséquent les deux notions ne sont pas identiques ; on verra § 4 les relations connues entre elles : en particulier qu'elles coïncident dans le cas d'un langage du premier ordre.

(ii) [D'après l'exercice 1 du Chap. 7], les principales structures étudiées au XIX[e] siècle (Arithmétique, Analyse) admettent une axiomatisation $\mathscr{A}_S$ qui satisfait $E^{\mathscr{A}_S}$ et $U^{\mathscr{A}_S}$. [S étant infini il faut que $\mathscr{A}_S$ soit d'ordre supérieur à 1 pour satisfaire $U^{\mathscr{A}_S}$.]

(iii) Notez que $U^{\mathscr{A}_S}$ et $E^{\mathscr{A}_S}$ sont formulés dans le langage ensembliste $\mathscr{L}_E$, langage du premier ordre dont l'unique symbole relationnel est $\in$, les variables variant sur les ensembles, et $\in$ désignant la relation d'appartenance (voir à la fin de ce paragraphe la modification de la notion de réalisation employée ici). Pour les structures classiques S, $E^{\mathscr{A}_S}$ et $U^{\mathscr{A}_S}$ sont démontrées à l'aide de propriétés familières des notions de base ensemblistes.

(iv) Par contre la vérification de $X^{\mathscr{A}_S}$ et $D^{\mathscr{A}_S}$, également faite pour les structures classiques, réclame une étude de chaque cas qui se présente dans la pratique, comme celle qui se trouve dans *Principia Mathematica.*

Evidemment $X^{\mathscr{A}_S}$ dépend de ce qu'on entend par « propriété mathématique de S » ; par exemple, en arithmétique on veut que soient exprimées dans le langage l'addition, la multiplication, etc., mais pas des propriétés « empiriques » comme le nombre d'électrons émis par un atome entre les temps n et $n + 1$.

(v) Si $U^{\mathscr{A}_S}$ et $X^{\mathscr{A}_S}$ sont satisfaites, alors aussi $D^{\mathscr{A}_S}$ (cf (i)). Mais même si $U^{\mathscr{A}_S}$ n'est pas vraie, une étude détaillée peut démontrer que $D^{\mathscr{A}_S}$ est vraie en regard de la pratique, en ce sens que toutes les propriétés de *S jusqu'ici démontrées* sont conséquences logiques de $\mathscr{A}_S$: cette possibilité est réalisée effectivement par des axiomatisations du 1[er] ordre de l'arithmétique, cf. B, p. 197.

(vi) Signalons que la notion d'isomorphisme utilisée pour $U^{\mathscr{A}_S}$ et pour la notion de « propriété purement logique » est exactement

la notion générale propre aux mathématiques pures. Mais que, dans les applications, deux structures abstraitement isomorphes peuvent ne pas présenter le même degré d'effectivité ; par exemple une structure S′ isomorphe à l'arithmétique (i. e. un autre système de notations des entiers) serait inutilisable pour compter si la relation de successeur était indécidable dans S'.

N. B. Les conditions d'adéquation ci-dessus sont établies pour les axiomatisations des structures classiques, mais non pour la structure de base F (F pour fondamental), collection de tous les ensembles, munie de la relation d'appartenance (ni pour la structure intuitive des ordinaux avec la relation d'ordre).

Car si $\mathscr{A}_F$ est une axiomatisation de F, $E^{\mathscr{A}_F}$ signifie l'existence d'une réalisation satisfaisant $\mathscr{A}_F$, dont l'univers est par définition un *ensemble*. Si alors $U^{\mathscr{A}_F}$ était vérifiée, cet ensemble aurait la puissance de la collection de tous les ensembles.

1. Résultats élémentaires sur la notion intuitive d'ordinal.

Pour formuler ces résultats, nous avons besoin de la notion *généralisée*, mentionnée plus haut, de réalisation, qui est explicitée ci-dessous dans le cas du langage $\mathscr{L}_E$ auquel sont adjoints les symboles de relation O, P, à une et deux variables respectivement :

Les variables n'ont pas pour domaine un ensemble, mais la collection de tous les ensembles.

L'interprétation d'un symbole de relation n'est pas nécessairement un ensemble, mais peut être une propriété d'ensembles (dans le cas de O) ou de couples d'ensembles (dans le cas de P). On notera $\bar{A}$ la propriété définie par une formule A, i. e., propriété de la satisfaire.

(Le lecteur comparera cette extension de la notion de réalisation avec la situation analogue suivante : dans cette parenthèse, la notion de base est celle d'ensemble (héréditairement) *fini*. La structure f de tous les ensembles finis n'admet pas d'axiomatisation adéquate $\mathscr{A}_N$, car vu la notion de base considérée, une « réalisation » de $\mathscr{A}_N$ a un univers fini. Il est donc nécessaire d'étendre pour f la notion de réalisation. Si donc on considère le langage $\mathscr{L}_E$ augmenté des symboles relationnels, N et S à une variable, resp. à deux variables, la structure suivante est une réalisation généralisée : l'univers est celui de f, $\bar{\in}$ est l'appartenance entre ensembles finis ; $\overline{N(x)}$ est la *propriété* d'ensembles « x est un entier naturel », i. e. :

$$x = 0 \vee \wedge y[\wedge z(z \cup \{ z \} \in y \to z \in y) \to (x \in y \to 0 \in y)] .$$

$\overline{S(x, y)}$ est la propriété « y est successeur de x », i. e. $y = x \cup \{x\}$, où on écrit $y = 0$ pour $\Lambda z \neg z \in y$ et $y = x \cup \{x\}$ pour

$$\Lambda z [z \in y \leftrightarrow (z = x \vee z \in y)].$$

Revenons au cas général ; nous voulons définir la réalisation au sens étendu, $\langle \overline{O}, \overline{P} \rangle$, des ordinaux avec leur ordre, i. e. satisfaire aux conditions suivantes :

les ordinaux sont des ensembles ;

(i) $\overline{P}$ est un ordre total de $\overline{O}$, i. e. $\Lambda xy[Pxy \leftrightarrow (Ox \wedge Oy \wedge x \neq y \wedge \neg Pyx)]$;

(ii) Tout segment initial de $\overline{O}$ est bien ordonné par la restriction de $\overline{P}$ [i. e. :

$$\Lambda x \{ Ox \rightarrow \mathrm{V} yz[\Lambda u(u \in y \leftrightarrow Pux) \wedge$$
$$\wedge \Lambda u \, \mathrm{V} st[(u \in z \leftrightarrow u = (s, t) \wedge s \in y \wedge t \in y \wedge Pst)] \wedge We(y, z)] \},$$

où (s, t) désigne le couple ordonné (voir Ex. 5 du Chap. 5) et où $We(y, z)$ signifie que z est bien fondée sur y, i. e.

$$\Lambda X \{ \mathrm{V} v([v \in y \wedge Xv] \rightarrow \mathrm{V} w[w \in y \wedge Xw \wedge$$
$$\wedge \Lambda w'([Xw' \wedge w' \in y \wedge w \neq w'] \rightarrow (w, w') \in z)]) \}$$

[X étant une variable de type (0) comme au Chap. 7].

(iii) Chaque couple (y, z), $z \subset y^2$, où z est un bon ordre sur y, est isomorphe à un segment de $\overline{O}$ ordonné par $\overline{P}$.

Ces axiomes sont suffisants pour déterminer $\langle \overline{O}, \overline{P} \rangle$ uniquement (à un isomorphisme près : juste comme les axiomes de Péano déterminent la structure de l'Arithmétique). Il y a des *formules* de $\mathscr{L}_E$ qui définissent $\overline{O}$ et $\overline{P}$ explicitement de façon à satisfaire (i), (ii), (iii) (exactement comme les propriétés $\overline{N}$ et $\overline{S}$ sont définies par les formules ci-dessus).

Pour plus d'information sur la théorie intuitive des ordinaux (et pour les quelques notations et propriétés qui sont utilisées plus loin), consultez par exemple E. KAMKE, *Théorie des ensembles*, Dunod.

Voici quelques notations utilisées par la suite dans les exercices :

$x = 0$	pour $\Lambda u \neg u \in x$.
$x = y \cup \{z\}$	pour $\Lambda w[w \in x \leftrightarrow (w \in y \vee w = z)]$.
$x = \{y\}$	pour $\Lambda u(u \in x \leftrightarrow u = y)$.
$x = \{y, z\}$	pour $x = \{y\} \cup \{z\}$.
$x = (y, z)$	pour $x = \{\{y\}, \{y, z\}\}$ (couple ordonné).
(y, z, w)	pour $((y, z), w)$.
Fonc (x)	pour

$$\Lambda z(z \in x \leftrightarrow \mathrm{V} vw[z = (v, w)]) \wedge \Lambda uvw([(u, v) \in x \wedge (u, w) \in x] \rightarrow v = w)$$

(graphe d'une fonction).

Dom (y, x) pour $\Lambda u[u \in y \leftrightarrow \mathrm{V} v((u, v) \in x)]$ (y domaine de x).

Pour chaque *chiffre* 1, 2, 3, ... on écrit $1 = \{0\}$, $2 = 1 \cup \{1\}$, $3 = 2 \cup \{2\}, \ldots$ (Cf. p. 163 la définition des entiers).

$Sf(x)$ pour Fonc $(x) \wedge \bigvee y[Ny \wedge \text{Dom}(y, x) \wedge y \neq 0]$ (x est une suite finie, i. e., une fonction dont le domaine est un entier > 0. N est défini page précédente.)

$x = Sub(y, z, v)$ pour

$$Sf(y) \wedge \bigwedge uw[(u, w) \in x \leftrightarrow ([(u, w) \in y \wedge w \neq z] \vee [(u, z) \in y \wedge w = v])]$$

(x est obtenue en substituant v à z dans la suite y).

$x + y = z$ pour

$$\bigvee w[Sf(w) \wedge Dom(x \cup \{x\}, w) \wedge (0, y) \in w \wedge$$
$$\wedge \bigwedge uv([u \in x \wedge (u, v) \in w] \to [(u \cup \{u\}, v \cup \{v\}) \in w]) \wedge (x, z) \in w]$$

[Cf Chap. 5, Ex. 7.]

$x = \widehat{yz}$ pour

$$Sf(y) \wedge Sf(z) \wedge \bigwedge u[u \in x \to (u \in y \vee \bigvee vwr[Dom(v, y) \wedge$$
$$\wedge u = (w + v, r) \wedge (w, r) \in z])]$$ (la concatenée de y et z).

$x = \widehat{y}$ pour $Sf(x) \wedge Sf(y) \wedge \bigvee w[Dom(w, x) \wedge$
$\wedge Dom(w, y)] \wedge$

$$\wedge \bigwedge uv[(u, v) \in y \to Sf(v)] \wedge \bigwedge u[(0, u) \in x \to (0, u) \in y] \wedge$$
$$\wedge \bigwedge uvw\{[(u, v) \in x \wedge (u \cup \{u\}, w) \in y] \to (u \cup \{u\}, \widehat{vw}) \in x\}$$

(accumulation d'une suite finie de suites finies).

2. Comment trouve-t-on des lois pour les notions de base ensemblistes ?

(Analyse conceptuelle de F.) Quelles que soient les réponses données par des analyses plus raffinées, la découverte de telles lois se présente naïvement comme suit :

l'on choisit un langage, en particulier $\mathscr{L}_E$, *et l'on y formule des assertions vraies pour la réalisation F.*

La sélection ainsi faite entre les assertions vraies est déterminée dans une certaine mesure par les « besoins » actuels des mathématiques ; par exemple, on choisit des assertions utilisées dans la démonstration de $U^{\mathscr{A}s}$ ou de $E^{\mathscr{A}s}$ pour les structures classiques. Mais on cherche aussi à formuler les propriétés générales essentielles, dont ces assertions sont des cas particuliers (cf note 4, p. 182).

Mais les mathématiciens demandent parfois : qu'est-ce que le vrai (pour les ensembles) ? Et (renouvelant Pilate), ils s'en lavent les mains. Sans nier l'intérêt de la question (toute la partie B est consacrée à *une* réponse détaillée), nous admettons ici la notion de vérité ensembliste — ce qui est implicite dans l'acceptation des notions de base ensemblistes — et nous recherchons ce qu'elle apporte à la théorie des fondements ; le problème de donner une justification aux axiomes se présente alors sous cette forme très naturelle : d'une façon générale, des axiomes sont justifiés du point de vue ensembliste si l'on détient un concept (précis) qui satisfait ces axiomes. En particulier, $\mathcal{A}_S$ est justifié si $E^{\mathcal{A}_S}$ est vrai.

Une autre justification de $\mathcal{A}_S$ est la dérivation formelle de $E^{\mathcal{A}_S}$ à partir des axiomes traditionnels de la théorie des ensembles à condition d'avoir justifié déjà ces axiomes, i. e., si l'on détient un concept précis d'ensemble, qui les satisfait. Les alinéas *b*) et *c*) sont consacrés à ce point.

a) Nécessité d'une analyse conceptuelle. — Bien avant que les paradoxes de la théorie des ensembles n'aient conduit aux restrictions sophistiquées sur les définitions d'ensembles (« prédicativité » de Poincaré) ou sur les méthodes de démonstration (constructivité de Brouwer), certaines ambiguïtés de la notion d'ensemble suscitèrent une première critique.

Cette critique n'est pas décisive, elle montre simplement la nécessité de certaines distinctions : la notion d'ensemble, telle qu'elle fut introduite, était un mélange grossier d'au moins trois éléments : les ensembles étaient considérés

(i) comme une vague extension de la notion de collection finie, obéissant plus ou moins aux mêmes lois (supposées connues),

(ii) comme des sous-collections arbitraires d'une collection donnée (supposée bien définie) : ceci était répandu dans toutes les mathématiques (ensembles d'entiers, de réels, etc.),

(iii) comme une abstraction tirée de la notion plus générale de propriété, un ensemble étant la collection des objets satisfaisant une propriété donnée. Les mathématiques elles-mêmes font peu usage de propriétés pour l'extension desquelles il n'y a pas à priori de limites, mais la logique générale et le langage courant s'en servent tous deux largement. Par exemple la propriété d'être non vide (remarquons que cette propriété s'applique à elle-même) ; ou la propriété d'être bleu, car même si son extension a une limite, nous utilisons cette propriété sans idée précise de la classe de toutes les choses bleues (passées, présentes et futures !).

L'intérêt possible pour les mathématiques de telles propriétés est envisagé à la fin de cet alinéa.

Des erreurs flagrantes (contradictions) dans l'utilisation mathématique des notions ensemblistes sont rares parce que, en général, une démonstration donnée est valable d'un bout à l'autre au moins pour l'une des trois notions d'ensembles ci-dessus. Mais si un raisonnement utilise des principes dont chacun est vérifié par l'une des notions, mais dont l'ensemble n'est vérifié par aucune des trois, ce raisonnement peut conduire à une contradiction : c'est le cas des erreurs connues sous le nom de paradoxes, erreurs particulièrement désagréables parce qu'elles ne peuvent pas être localisées en un endroit unique comme des erreurs de calcul. Il est clair que, pour l'analyse correcte de ces erreurs, et même pour la formulation de cette analyse, les distinctions mentionnées sont nécessaires.

Exemple (Axiome de compréhension). — Si P est une propriété définie sur les éléments d'un ensemble donné, a, on peut former l'ensemble, au sens de (ii) de tous les x de a qui satisfont P, i. e. :

(*) $\bigwedge a \bigvee y \bigwedge x[x \in y \leftrightarrow (x \in a \wedge Px)]$.

Russell remarqua, en fait si longtemps après l'introduction de la théorie des ensembles que l'impression naïve d'ambiguïté avait été oubliée, que

(**) $\bigvee y \bigwedge x(x \in y \leftrightarrow Px)$

est *contradictoire* si l'on applique les règles ordinaires de logique ; en particulier si Px est la propriété $x \notin x$, (**) est $\bigvee y \bigwedge x\,(x \in y \leftrightarrow x \notin x)$, et alors $y \in y \leftrightarrow y \notin y$ ce qui est une contradiction.

(ii) Mais dès avant cette remarque, (**) n'était pas du tout plausible et certainement pas évident pour la notion d'ensemble.

Pour la notion (iii), $x \in y$ étant interprété comme : la propriété x a la propriété y, (**) est *évident* pourvu que l'on considère la sorte la plus générale de propriété, comprenant des propriétés qui ne sont pas partout définies. Alors, (**) exprime que y est une propriété satisfaite par une propriété x si, et seulement si x est satisfaite par elle-même ; mais cette propriété y n'est pas définie pour l'argument y. Mais dans ce cas les lois usuelles de la logique formelle [qui sont valides pour l'interprétation des symboles logiques du Chap. 2] ne peuvent pas être valides : on ne peut avoir pour tout A, ou bien A est (défini et) vrai ou bien A est (défini et) faux.

Il est clair que le paradoxe de Russell (ou n'importe quel autre) n'affecte pas plus la notion d'ensemble au sens de (ii) qu'il n'affecte, par exemple, la notion d'ensemble héréditairement fini, construit à partir de ϕ. (Dans ce cas (**) est évidemment faux, quand on prend pour Px « $x \notin x$ » ou bien « x est un entier », et que x, y varient sur les ensembles finis. Et par contre (*) est valide lorsque toutes les variables varient sur les ensembles héréditairement finis.)

Néanmoins à propos du paradoxe de Russell, il se pose encore aujourd'hui une question qui est le *problème contemporain des paradoxes* :

Est-ce que la notion (iii) est assez précise pour permettre une théorie aussi riche que celle de (ii) qui est donnée en *b*) ci-dessous? En particulier, quelles sont ses lois logiques ? Et si cette théorie est riche, est-elle importante pour la pratique mathématique, ou seulement pour la théorie des fondements ?

Discussion (reliant ce qui précède à certaines remarques générales de l'introduction).

Les distinctions (i)-(iii) ci-dessus constituent un exemple de *précision informelle*. La discussion de l'axiome de compréhension illustre la manière dont de telles distinctions informelles servent l'établissement d'axiomes corrects tels que (*). Le lecteur observera que la formulation explicite de (*) n'était pas un moyen en quelque sorte tombé du ciel pour préciser la notion de base d'ensemble, mais au contraire le résultat d'une clarification informelle. En ce qui concerne (**), sa formulation explicite a certainement servi à mettre en évidence l'imprécision du mélange grossier qu'était la notion originelle d'ensemble, mais de nouveau, la discussion informelle de (iii) était nécessaire pour montrer qu'au moins (**) était plausible à priori.

De façon générale, la formulation explicite (formalisation) peut servir à découvrir par où certaines idées pèchent, mais ne joue au mieux qu'un rôle auxiliaire quand il s'agit de les rectifier.

Le passage de distinctions informelles (et plus généralement de la réflexion sur le sens d'un concept) à la formulation d'axiomes est appelé *dérivation informelle*. Le lecteur devrait mettre en balance l'exemple ci-dessus de dérivation informelle, et la doctrine positiviste citée en fin de l'introduction, qui considère les dérivations informelles soit comme vides de sens, soit au moins comme non mathématiques.

Notez pour finir, que le choix *entre* les diverses notions isolées par l'analyse informelle n'est pas forcément arbitraire. Ainsi, dans le cadre « réaliste » des fondements, des considérations de définissabilité donnent un critère (partiel) selon lequel, de deux groupes x, y de notions, le groupe x est le plus fondamental si y peut se définir à partir de x et non l'inverse. Ainsi la notion (ii) est plus fondamentale que celle d'ensemble fini.

Il est plausible que, si la notion d'ensemble (iii) s'avère précise, elle soit plus fondamentale que (ii).

Bien sûr, il ne faut pas supposer que les notions fondamentales pour une théorie réaliste nous doivent être particulièrement accessibles.

b) Existence d'une notion précise d'ensemble. (Ensemble au sens de (ii) satisfaisant (*)). — Peu après la publication du paradoxe de Russell, Russell

et Zermelo formulèrent tous deux la notion précise d'ensemble, appelée théorie des types.

La version de Zermelo, dite structure cumulative des types (s. c. t.) [voir l'Ex. 5 du Chap. 5], est la suivante : C_0 est une collection d'individus, i. e. d'objets x qui satisfont $\bigwedge y(\neg\, y \in x)$ (C_0 peut être vide).

Pour tout ordinal α, $\qquad C_{\alpha+1} = C_\alpha \cup \mathfrak{P}(C_\alpha)$,

Pour un ordinal limite α, $\quad C_\alpha = \bigcup_{\beta<\alpha} C_\beta$,

où $\mathfrak{P}(x)$ désigne la collection de toutes les parties de x. Donc, à côté des opérations logiques sur les ensembles, la définition de cette structure utilise l'opération supplémentaire $\mathfrak{P}$, et son *itération* (jusqu'à tout ordinal α dont on suppose l'existence).

DÉFINITIONS : On appelle *type* d'un ensemble x le plus petit α tel que $x \in C_\alpha$. On note $\in_\alpha$ la relation d'appartenance sur la s. c. t., restreinte à C_α.

La formule (**) est *évidemment fausse* dans la structure $\langle C_\alpha, \in_\alpha \rangle$, pour tout α (i. e. quand les variables ont C_α pour domaine), si l'on choisit par exemple pour propriété $Py : y = y$; en effet $C_\alpha \notin C_\alpha$.

La formule (*) est *évidemment vraie* pour tout α. Zermelo a énoncé des axiomes donnés en *c*) ci-dessous, qui sont la base de tous les systèmes d'axiomes habituels de la théorie des ensembles, et qui de plus sont satisfaits par $\langle C_\alpha, \in_\alpha \rangle$ pour tout ordinal limite α. Ainsi, comme ce résultat se voit très facilement, la notion précise d'ensemble est une preuve de consistance pour ces axiomes (cf. p. 165), particulièrement pour de petits ordinaux α tels que $\omega + \omega$ ou $\omega + \omega + \omega$.

c) Axiomes de Zermelo. — Le lecteur devrait vérifier qu'ils sont satisfaits dans $\langle C_\alpha, \in_\alpha \rangle$ pour les valeurs de α indiquées :

Extensionnalité (tout α) .

Si $y \subset x$ signifie : $\bigwedge u(u \in y \to u \in x)$.

1. $\bigwedge x \bigwedge y \{ \bigvee z(z \in x) \to [(y \subset x \wedge x \subset y) \to (x = y)] \}$.

Si la condition $\bigvee z(z \in x)$ (x n'est pas un individu, x n'est pas vide) est supprimée, l'axiome obtenu est encore satisfait par la s. c. t. si C_0 est vide.

Ensemble des parties (α limite)

2. $\bigwedge x \bigvee y \bigwedge z(z \in y \leftrightarrow z \subset x) \qquad (x \in C_\beta \to y \in C_{\beta+1})$

Compréhension (tout $\alpha > 0$)

3. $\bigwedge X \bigwedge a \bigvee x \bigwedge y[y \in x \leftrightarrow (y \in a \wedge X(y))]$

X est une variable de second ordre et l'on ne considère que des modèles principaux (cf. Chap. 7). 3 exprime ce qui est réellement visé par (*) et permet une démonstration particulièrement simple de résultats de base comme le théorème 1 ci-dessous. Cependant, on utilise couramment des systèmes d'axiomes du premier ordre en raison de la possibilité de formaliser les déductions à partir de tels systèmes (cf. ci-dessous Lemme 3 p. 176, ou § 4).

3 est alors remplacé par un schéma d'axiomes, c'est-à-dire restreint à des X qui sont la réalisation d'une formule de $\mathscr{L}_E$:]

3*. Pour toute formule $A(y, x_1, .., x_n)$ ne contenant pas la variable x, on prend comme axiome :

$$\wedge a \wedge x_1 \ldots \wedge x_n \vee x \wedge y(y \in x \leftrightarrow [y \in a \wedge A(y, x_1, \ldots, x_n)]) .$$

Axiomes des paires (α limite) *et de l'union* (tout $\alpha > 0$) :

4*. $\wedge x_1 \wedge x_2 \vee x \wedge y[y \in x \leftrightarrow (y = x_1 \vee y = x_2)]$,

5*. $\wedge z \vee x \wedge y[y \in x \leftrightarrow \vee u(u \in z \wedge y \in u)]$.

Régularité (tout α)

Chaque structure $\langle C_\alpha, \in_\alpha \rangle$ étant construite par itération transfinie à partir d'un ensemble d'*individus*, la relation est bien fondée, ce qui s'exprime par « l'axiome de régularité » :

6. $\wedge X \{ (\vee z X z) \rightarrow \vee x \wedge y[Xx \wedge (Xy \rightarrow y \notin x)] \}$.

De nouveau, au premier ordre, on utilise ce schéma, conséquence de 6 :]

6*. Pour toute formule $A(x)$, $\vee z A(z) \rightarrow \vee x \wedge y[A(x) \wedge (A(y) \rightarrow y \notin x)]$.

Les axiomes 1, 2 [3, 6 et par conséquent] 3*, 4*, 5*, 6*, sont satisfaits par $\langle C_\omega, \in_\omega \rangle$. Quand $C_0 = 0$, tous les ensembles de cette structure sont héréditairement finis. Cette possibilité est exclue par l'axiome :

Axiome de l'infini ($\alpha > \omega$) .

7. $\vee x\, I_1 x$, où $I_1 x$ est :

$$\vee y(y \in x) \wedge \wedge z \{ (z \in x) \rightarrow \vee w[w \in x \wedge \wedge u[u \in w \leftrightarrow (u \in z \vee u \subset z)]] \} .$$

Notations : [(1, 2, 3, 7) est noté $\mathscr{A}$ et] (1, 2, 3*, 4*, 5*, 7) est noté $\mathscr{A}^*$. Le système d'axiomes $\mathscr{A}^*[\mathscr{A}]$ sans axiome de l'infini sera noté $\mathscr{A}^*_-[\mathscr{A}_-]$.

Ainsi 1, 2, 7 [3, 6 et par conséquent] 3*, 4*, 5*, 6* étant satisfaits par $\langle C_\alpha, \in_\alpha \rangle$ pour tout α limite $> \omega$, [$E^{\mathscr{A}}$ est vraie, et] $E^{\mathscr{A}^*}$ est vraie.

Exercice 1. On utilisera les notations p. 163 et, pour toute formule Ax ne contenant pas la variable y, on notera $\bigvee!xAx$ la formule $\bigvee x \bigwedge y[A(y) \leftrightarrow x = y]$ (lire : il existe un seul x tel que Ax). Vérifier que

a) $\bigwedge yz \bigvee!x\,(x = y \cup \{z\})$ est conséquence des axiomes 1 et 4*,

b) pour tout triplet de chiffres n, m, p ou bien $n + m = p$ est conséquence de $\mathscr{A}^*_-$ ou bien $n + m \neq p$ est conséquence de $\mathscr{A}^*_-$.

c) $\bigwedge yzv\,[Sf(y) \to \bigvee!x\,(x = Sub\,(y, z, v))]$, $\bigwedge yz\,[(Sf(y) \wedge Sf(z))] \to \to \bigvee!x\,(Sf(x) \wedge x = \widehat{yz})]$, $\bigwedge y\,[Sf(y) \to \bigvee!x\,(Sf(x) \wedge x = \widehat{y})]$ sont conséquences de $\mathscr{A}^*_-$.

Démontrer que $\bigwedge x[(Sf(x) \wedge Nx) \to Dom\,(1, x)]$ est conséquence de 1 et 4* [(*a*)-(*c*) montrent que, d'après l'Ex. 6 du Chap. 5, les symboles fonctionnels introduits p. 163-164 peuvent être éliminés au sens qui y est précisé].

d) Est-ce que les axiomes de Zermelo axiomatisent la s. c. t. au sens du § 1? [$U^{\mathscr{A}}$ est faux, donc] $U^{\mathscr{A}^*}$ est faux, puisque, si $\alpha < \beta$, card $C_\alpha <$ card C_β.

Les résultats ci-dessous montrent que, relativement à la s. c. t., [ni $X^{\mathscr{A}}$ ni $D^{\mathscr{A}}$ ne sont satisfaits, et donc :] ni $X^{\mathscr{A}^*}$, ni $D^{\mathscr{A}^*}$, ne sont satisfaits.

$D^{\mathscr{A}^*}$ est réfuté sous la forme remarquable que $E^{\mathscr{A}^*}$ n'est pas conséquence de $\mathscr{A}^*$, i. e. on ne peut prouver au moyen de $\mathscr{A}^*$ que $\mathscr{A}^*$ a un modèle. [De même $E^{\mathscr{A}}$ n'est pas conséquence de $\mathscr{A}$.]

Les résultats précédant le théorème 4 sont techniquement simples. Ils éclairent la situation, et en plus montrent l'utilité de l'interprétation des axiomes de Zermelo par $\langle C_\alpha, \in_\alpha \rangle$.

[Théorème 1. — *$E^{\mathscr{A}}$, $E^{\mathscr{A}_-}$ ne sont pas conséquences de $\mathscr{A}$, $\mathscr{A}_-$ respectivement.*

Soient $M = \langle C_{\omega+\omega}, \in_{\omega+\omega} \rangle$ et $M_- = \langle C_\omega, \in_\omega \rangle$, avec $C_0 = \phi$; M et M_- sont les modèles minimaux de $\mathscr{A}$ et $\mathscr{A}_-$ resp. — Posons $\aleph^{(0)} = \aleph_0$ et pour tout entier n, $\aleph^{(n+1)} = 2^{\aleph^{(n)}}$. Alors card $C_{\omega+n} = \aleph^{(n)}$ et donc

$$\text{card } M = \sum_n \aleph^{(n)}\,.$$

Donc tout modèle de $\mathscr{A}$ a une cardinalité supérieure ou égale à $\sum \aleph^{(n)}$. Et tout modèle de $\mathscr{A}_-$ est infini car il contient C_ω.

$E^{\mathscr{A}}$ est faux dans M puisque tout élément de M a une cardinalité $< \sum \aleph^{(n)}$; $E^{\mathscr{A}_-}$ est faux dans M_- puisque tout élément de M_- est fini.

$E^{\mathscr{A}}$ et $E^{\mathscr{A}_-}$ ne sont même pas conséquences de ($\mathscr{A}$, 6) et ($\mathscr{A}_-$, 6) resp., parce que M et M_- satisfont 6. (Pour les structures S classiques, $E^{\mathscr{A}s}$ et $U^{\mathscr{A}s}$ sont déjà conséquences de $\mathscr{A}^*$!).]

Théorème 2. — *$E^{\mathscr{A}^*_-}$ n'est pas conséquence de $\mathscr{A}^*_-$.*

[Ce résultat plus faible que le théorème 1 est cependant détaillé, parce qu'il

n'est pas supposé de tout lecteur connaissance de la notion de conséquence du second ordre.]

Toute structure $\langle a, b \rangle$, où $b, \subset a^2$, est l'interprétation de $\in$, qui satisfait $\mathscr{A}^*_-$, contient une sous-structure isomorphe à $\langle C_\omega, \in_\omega \rangle$, donc est infinie. Mais toute structure $\langle a, b \rangle$, où $b \subset a^2$, et a et $b \in C_\omega$, est finie. Donc $E^{\mathscr{A}^*_-}$ est fausse dans $\langle C_\omega, \in_\omega \rangle$.

Par contre $\langle C_\omega, \in_\omega \rangle$ satisfait $(\mathscr{A}_-, 6)$. Donc $E^{\mathscr{A}^*_-}$ n'est pas conséquence de $(\mathscr{A}^*_-, 6)$ à fortiori de $\mathscr{A}^*_-$.

Un premier échec de $D^{\mathscr{A}^*}$ est que les axiomes ne disent rien sur la possibilité de construire $\langle C_\alpha, \in_\alpha \rangle$ pour $\alpha > \omega + \omega$:

THÉORÈME 3. — *Les axiomes [$\mathscr{A}$ ou] $\mathscr{A}^*$ ne sont pas saturés,* i. e. *il existe une formule I_2 telle que ni I_2 ni sa négation ne soient conséquences de [$\mathscr{A}$ ou] $\mathscr{A}^*$.*

$$I_2 = \bigvee y[\bigvee x(I_1 x \wedge x \in y) \wedge \bigwedge z(z \in y \rightarrow \mathfrak{P} z \in y)]$$

où « $\mathfrak{P} z \in y$ » signifie $\bigvee w \{ w \in y \wedge \bigwedge u [u \in w \leftrightarrow (u \in z \vee u \subset z)]\}$.

I_2 exprime l'existence d'ensembles de type $\omega + \omega + 1$.

Les axiomes sont satisfaits par $\langle C_{\omega+\omega}, \in_{\omega+\omega} \rangle$ et par $\langle C_{\omega+\omega+\omega}, \in_{\omega+\omega+\omega} \rangle$; $\neg I_2$ est satisfait dans le premier cas, I_2 dans le deuxième.

On notera que la formule I_2, du premier ordre, n'est même pas une conséquence du second ordre de $\mathscr{A}$.

Ces résultats simples vont être puissamment généralisés et renforcés par une démonstration différente : généralisés à d'autres systèmes que $\mathscr{A}^*$, et renforcés en démontrant la non-saturation pour des assertions beaucoup plus élémentaires que I_2. C'est le théorème d'incomplétude de Gödel :

THÉORÈME 4. — *$E^{\mathscr{A}^*}$ n'est pas conséquence de $\mathscr{A}^*$.*

Remarques : (i) La démonstration n'utilise qu'une faible partie des propriétés de $\mathscr{A}^*$: pour qu'un système d'axiomes soit substituable à $\mathscr{A}^*$ dans le théorème il suffit qu'il vérifie des conditions très générales — dont la formulation précise exigerait des notions de la théorie des fonctions récursives, qui n'est pas traitée dans ce livre.

Un exemple de système d'axiomes auquel la démonstration ne s'applique pas est : $\mathscr{A}_T = \{A : A$ est dans le langage $\mathscr{L}_E$, et $\overline{A}$ est vrai dans la s. c. t. $\}$, car ce système est évidemment complet. Mais on ne peut même pas définir l'ensemble $\mathscr{A}_T$ à l'aide d'une formule de $\mathscr{L}_E$ (cf. corollaire 1 ci-dessous).

(ii) En divers endroits — en particulier aux lemmes 4 et 5 —, il est démontré que certaines formules de $\mathscr{L}_E$ sont satisfaites par la s. c. t., et il est seulement affirmé sans démonstration détaillée que ces formules sont en fait conséquences de $\mathscr{A}^*$, parce que leur démonstration, qui est simple, n'utilise que des propriétés de $\mathscr{A}^*$. Sachant que certaines formules vraies dans la s. c. t. ne sont pas conséquences de $\mathscr{A}^*$ (par exemple $E^{\mathscr{A}^*}$!) on peut mettre en doute cette affirmation.

Mais dans tous les cas : *ou bien* le théorème 4 est vrai ; *ou bien* $D^{\mathscr{A}^*}$ est faux parce que ces raisonnements intuitifs ne sont pas conséquences logiques de $\mathscr{A}^*$, *ou enfin* $X^{\mathscr{A}^*}$ est faux comme $X^{\mathscr{A}_T}$ dans la remarque (i). Pour l'usage qui sera fait ci-dessous du théorème, ces conclusions plus faibles suffisent.

(iii) Les notions et propriétés syntaxiques élémentaires sont exprimables dans $\mathscr{L}_E$ et démontrables au moyen de $\mathscr{A}^*$ (cf. Exercices 2 et 3) : sinon $X^{\mathscr{A}^*}$ et $D^{\mathscr{A}^*}$ seraient réfutés.

Nous utilisons en particulier les propriétés suivantes : tous les objets syntaxiques (cf. Chap. 0) sont considérés comme des ensembles, car ce sont des suites ordonnées de symboles, et les symboles *sont* des ensembles ;

chaque symbole s du langage est supposé défini par une formule $C_s(t)$, c'est-à-dire que ce symbole est l'unique ensemble satisfaisant C_s dans s. c. t. De même chaque formule A est supposée définie par une formule $C_A(t)$.

N. B. Dans le lemme 2 la seule propriété utile de C_A est qu'elle définit l'ensemble A dans s. c. t. Mais si l'on veut que des propriétés syntaxiques simples soient conséquences de $\mathscr{A}^*$, un choix *canonique* de C_A est nécessaire. Par exemple, si $C_0(t)$ est $\bigwedge y \neg\, y \in t$, $(\bigvee ! t)\, C_0(t)$ est conséquence de $\mathscr{A}^*$. Mais supposez que P, quoique vraie dans s. c. t., n'est pas conséquence de $\mathscr{A}^*$; alors $P \wedge C_0$ définit 0 (dans s. c. t.), mais $\bigvee ! t[P \wedge C_0(t)]$ n'est pas conséquence de $\mathscr{A}^*$. [On comparera avec les notions de définissabilité, Chap. 6.]

(iv) Un caractère inhabituel de la démonstration est que des relations entre des formules et leur signification (c'est-à-dire leur réalisation au sens de la p. 160) y sont considérées, tandis que dans la plus grande partie des mathématiques, les démonstrations portent du début à la fin soit sur les formules, soit sur leur signification. [Exception : la définition de réalisation d'une formule, Chap. 2.] Les notations distinguent ces deux aspects : nous utilisons une barre au-dessus d'une formule quand il s'agit de sa réalisation dans s. c. t. ; ainsi, si A est une formule close, i. e. sans variable libre, $\bar{A}$ signifie que A est vraie dans s. c. t.

Le lecteur devra se rappeler quelques sous-entendus dans l'usage habituel des notations concernant un langage formel. Chacune des expressions A et Ax, ou encore $A(x)$, désignera la même suite de symboles de $\mathscr{L}_E$, $A(x)$ étant utile pour indiquer que A contient la variable (désignée par) x et que $A(t)$ est obtenue en remplaçant x dans A par l'expression (désignée par) t.

Dans les Exercices 2, 3 ci-dessous, on considérera pour fixer les idées « le » langage $\mathscr{L}_E$ constitué par les symboles suivants : les symboles relationnels, notés $=$ et $\in$, *sont* les entiers 0, resp. 1 ; les symboles « logiques », notés $\neg$, $\wedge$, $\bigvee$ sont 2, 3, 4 ; et les variables sont les entiers 5, 6, 7, ..., notés aussi v_0, v_1, v_2, ... ; v_n désigne donc l'entier $n + 5$.

Exercice 2. Démontrer que l'entier n est le seul objet qui satisfasse la formule E_n à une seule variable v_{4_n}, E_n définie par récurrence :

$$E_0 = \neg \bigvee v_2(v_2 \in v_0)$$

$$E_{n+1} = \bigvee v_{4n} \{ E_n \wedge \bigwedge v_{4n+6}[v_{4n+6} \in v_{4n+4} \leftrightarrow (v_{4n+6} = v_{4n} \vee v_{4n+6} \in v_{4n})]\} .$$

Démontrer que la suite finie $< n_0, ..., n_{k-1} >$ d'entiers est le seul objet s qui satisfasse

$$\bigvee x_0 ... \bigvee x_{k-1} \bigvee y_0 ... \bigvee y_k[E_{n_0}(x_0) \wedge \cdots \wedge E_{n_{k-1}}(x_{k-1}) \wedge E_0(y_0) \wedge \cdots \wedge \wedge E_k(y_k) \wedge Sf(s) \wedge \text{Dom}\,(y_k, s) \wedge (y_0, x_0) \in s \wedge \cdots \wedge (y_{k-1}, x_{k-1}) \in s]$$

où les x_i et les y_i désignent des variables, c'est-à-dire des entiers > 4, distinctes deux à deux, variables qui n'ont aucune occurrence liée dans la formule (désignée par) :

$$E_{n_0}(x_0) \wedge \cdots \wedge (y_{k-1}, x_{k-1}) \in w .$$

Remarque. — Le choix des E_n est lié au besoin (du Lemme 1) d'avoir deux variables qui ne figurent dans aucune définition canonique, la formule ci-dessus étant la définition canonique de la suite $\langle n_0, ..., n_{k-1} \rangle$, et n'utilisant pas les variables v_1 et v_3.

Pour être précis on devrait spécifier aussi les variables notées u, v, w, r, p. 163. Nous supposons que les variables v_1 et v_3 n'y sont pas comprises. [Le lecteur du Chap. 2 se rappellera que les parenthèses ne font pas partie du langage $\mathscr{L}_E$ et E_0 désigne donc $\neg \bigvee v_2 \in v_2\, v_0$, c'est-à-dire la suite d'entiers $\langle$ 2 4 7 1 7 5 $\rangle$.]

D'après l'exercice ci-dessus on voit facilement qu'il y a une formule $Def(y, x)$ de $\mathscr{L}_E$ qui définit dans s. c. t. la relation suivante : *x est une suite finie d'entiers et y est la formule de $\mathscr{L}_E$* (construite d'après le schéma de l'Ex. 2), *définissant x* [définition explicite dans $\mathscr{A}^*$ de relations définies par récurrence ; voir l'Ex. 6 du Chap. 5].

Si $\bar{x}$ est une formule A donnée et $\overline{Def(y, x)}$ est vrai, $\bar{y}$ est la formule $C_A(w)$.

Notations : Comme le lecteur aura observé, l'absence de symboles fonctionnels exige que les objets soient définis dans $\mathscr{L}_E$ par des *formules* et non par des *termes* (en contraste avec le langage $\mathscr{L}_C$ de la Partie B, § 2). Pour plus de clarté nous ajoutons à $\mathscr{L}_E$ des *constantes* $\ulcorner A \urcorner$, $\ulcorner B(\ulcorner A \urcorner) \urcorner$, pour tout couple de formules A et $B(x)$ de $\mathscr{L}_E$; et, pour toute formule $C(y)$ de $\mathscr{L}_E$, nous notons $C(\ulcorner A \urcorner)$ et $C(\ulcorner B(\ulcorner A \urcorner) \urcorner)$ les formules $\bigvee y[C_A(y) \wedge C(y)]$ resp.

$$\bigvee y[C_{B_1}(y) \wedge C(y)],$$

où B_1 désigne $\bigvee x[C_A(x) \wedge B(x)]$: autrement dit, la réalisation $\overline{\ulcorner A \urcorner}$ *est* la formule A et la réalisation $\overline{\ulcorner B(\ulcorner A \urcorner) \urcorner}$ est la formule B_1.

Dans les lemmes 4 et 5 ci-dessous on aura besoin de la fonction $F_A(\bar{x}_1, \bar{x}_2, \bar{x}_3)$, pour une formule A de $\mathscr{L}_E$ à trois variables, soit $A(x_1, x_2, x_3)$. Si $\bar{x}_1, \bar{x}_2, \bar{x}_3$ sont des suites d'entiers K, L, resp. M, la valeur de $F_A(\bar{x}_1, \bar{x}_2, \bar{x}_3)$ est, par définition, la formule de $\mathscr{L}_E$:

$$\bigvee w_1\, w_2\, w_3[C_K(w_1) \wedge C_L(w_2) \wedge C_M(w_3) \wedge A(w_1, w_2, w_3)]$$

où w_1, w_2, w_3 désignent trois variables distinctes qui ne figurent pas dans la formule A ni dans

$$C_K(w) \wedge C_L(w) \wedge C_M(w) .$$

On définit facilement F_A à partir de la relation *Def* et de la fonction *Sub* (p. 164) ; $C_K(w)$, $C_L(w)$, $C_M(w)$ étant les ensembles $\bar{y}_1$, $\bar{y}_2$, resp. $\bar{y}_3$ tels que $(\bar{x}_1, \bar{y}_1)$, $(\bar{x}_2, \bar{y}_2)$, $(\bar{x}_3, \bar{y}_3)$ satisfassent $\overline{Def}$.

Dans toute la démonstration on suppose que x et y sont deux variables fixées et distinctes, par exemple v_1 et v_3 (cf. la remarque de l'exercice 2), et qu'aucune variable des formules considérées n'a à la fois d'occurrences libres et liées.

LEMME 1. — *Pour toute formule $A(x)$ dans $\mathscr{L}_E$, il existe une formule close A_1 de $\mathscr{L}_E$ telle que :*

$$\overline{A_1 \leftrightarrow \neg A(\ulcorner A_1 \urcorner)} .$$

Démonstration. — On obtient d'abord une formule $S(x, y)$ de $\mathscr{L}_E$, dont la réalisation dans s. c. t. est la relation suivante :
il existe une formule $B(y)$ de $\mathscr{L}_E$ telle que $\bar{y} = B(y)$ et $\bar{x} = B(\ulcorner B \urcorner)$, (i. e. : $\bar{x}$ est la formule $\bigvee y[C_B(y) \wedge B(y)]$).

Posons alors

$$H(y) = \bigvee x[S(x, y) \wedge \neg A(x)] .$$

Pour toute formule $B(y)$,

$$\overline{H(\ulcorner B \urcorner) \leftrightarrow \neg A(\ulcorner B(\ulcorner B \urcorner) \urcorner)} .$$

Donc visiblement $A_1 = H(\ulcorner H \urcorner)$ convient.
En fait pour toute formule A, la formule $A_1 \leftrightarrow \neg A(\ulcorner A_1 \urcorner)$ est *conséquence de $\mathscr{A}^*$.*

[**Exercice 3** : Définition de la formule $S(x, y)$ du lemme 1.

Form (x) : x est une formule de $\mathscr{L}_E$ (et aucune variable n'a à la fois d'occurrences libres et liées dans x). Partant de la « définition par récurrence » des formules de $\mathscr{L}_E$ on obtient, d'après la méthode courante, une définition explicite telle que la formule de récurrence soit conséquence de $\mathscr{A}^*$.

$Vl(v, x)$: v est la seule variable libre de la formule x (et toutes ses occurrences sont libres), i. e.

$$Vl(v, x) = Form(x) \wedge N(v) \wedge 4 \in v \wedge \bigwedge u\,[(u, 4) \in x \rightarrow$$
$$\rightarrow (u \cup \{u\}, v) \notin x] \wedge \bigwedge u \bigwedge w\{[N(u) \wedge 4 \in u \wedge u \neq v \wedge$$
$$\wedge (w, u) \in x] \rightarrow \bigvee y[(y, 4) \in x \wedge y \in w \wedge (y \cup \{y\}, u) \in x]\}.$$

(Puisque v est une variable, $N(v) \wedge 4 \in v$ est vrai, c'est-à-dire, v est un entier > 4 ; puisque v est libre, v n'est pas précédé par un quantificateur, i. e., par 4 ; et puisque v est la seule variable libre, toute autre variable, i. e., tout autre entier $u > 4$ dans la suite x, a sa première occurrence précédée par 4.)

$S(x, y)$: x est une formule à une seule variable libre, disons m, x a donc une définition canonique, disons z, dont la seule variable libre est, disons p ; on prend une variable q qui ne figure ni dans x ni dans z, p. ex. la première dans la suite $v_0, v_1, \ldots$ (i. e. 5, 6, ...) et on la substitue à m dans x et à p dans z, on obtient ainsi x', resp. z' : y est la suite $4\frown q \frown 3 \frown z' \frown x'$ ou encore $\bigvee v_N[Z(v_N) \wedge X(v_N)]$, où $Z(v_N)$ est la formule notée $C_X(v_N)$ ci-dessus ($X = \overline{x}$).]

Corollaire 1. — *Le lemme* 1 *réfute déjà* $X^{\mathscr{A}^*}$, *et même* $X^{\mathscr{A}_F}$ *pour tout axiome* $\mathscr{A}_F$ *dans* $\mathscr{L}_E$.

En effet, l'ensemble :

$$t = \{A : A \text{ est une formule close de } \mathscr{L}_E \text{ et } \overline{A} \text{ est vrai dans s. c. t.}\}$$

n'est la réalisation d'aucune formule $A(x)$ de $\mathscr{L}_E$; car si $t = \overline{A(x)}$, la formule A_1 du lemme 1 entraîne contradiction. Ceci est une remarque de Iarski.

Par contre, il existe une formule $V(x)$ telle que $\overline{V(x)}$ soit l'ensemble des formules closes conséquences ensemblistes de $\mathscr{A}^*$ (donc aussi conséquences au sens ordinaire. Cf. p. 160-161) [il suffit de formaliser la définition, du Chap. 2, de conséquence d'un axiome]. C'est pourquoi :

Lemme 2. — *Si* V_1 *est la formule déduite de* $V(x)$ *par le lemme* 1, $\overline{V_1}$ *est vrai, mais* V_1 *n'est pas conséquence de* $\mathscr{A}^*$.

$\overline{V_1 \leftrightarrow \neg V(\ulcorner V_1 \urcorner)}$, i. e. $\overline{V_1}$ est vraie si, et seulement si, V_1 n'est pas conséquence de $\mathscr{A}^*$. Comme toutes les conséquences de $\mathscr{A}^*$ sont vraies dans s. c. t. le résultat est démontré.

[*N. B.* Soit $\mathscr{A}_F$ un système d'axiome d'ordre $i > 1$, par exemple $\mathscr{A}_-$ ou $\mathscr{A}$. Soit V^i une formule (du premier ordre) dont la réalisation est l'ensemble des formules closes conséquences d'ordre i de $\mathscr{A}_F$. *Le lemme* 2 *s'applique à* $\mathscr{A}_F$ *et* V^i.]

Corollaire 2. — V_1 *n'est pas décidée par* $\mathscr{A}^*$, i. e. *ni* V_1 *ni* $\neg V_1$ *ne sont conséquences de* $\mathscr{A}^*$.

Pour renforcer ce résultat d'indécidabilité nous allons définir $D(x)$, aussi *élémentaire* que possible, telle que $\overline{D(x)} = \overline{V(x)}$, afin d'appliquer le lemme 2 en substituant D à V, D_1 à V_1.

Les principales propriétés de D vont être décrites ici. Mais leur démonstration (en particulier celle que $\overline{D} = \overline{V}$), et même l'énoncé précis de D, utilisent le Chap. 2.

(i) L'énoncé de D est obtenu de la façon suivante : la démonstration du lemme 3 fournit une « règle de déduction » particulière, analogue aux règles mentionnées p. 160, note 3, et montre que l'ensemble des formules de $\mathscr{L}_E$ déduites de $\mathscr{A}^*$ conformément à cette règle est $\overline{V}$; cette règle s'exprime dans $\mathscr{L}_E$, c'est-à-dire il existe une formule $Dem\ (y, x) \in \mathscr{L}_E$, telle que $\overline{Dem}$ est la relation (entre la suite finie de formules $\bar{y}$ et la formule $\bar{x}$) : « $\bar{y}$ est une déduction de $\bar{x}$ à partir de $\mathscr{A}^*$, conformément à la règle ».
Alors $D(x)$ est : $\mathsf{V}y\ Dem\ (y, x)$.

(ii) D est plus élémentaire que V en ce sens que ses quantificateurs sont restreints à C_ω (lorsque $\mathscr{L}_E$ et sa syntaxe sont définis comme dans les exercices), alors que certains quantificateurs de V ne sont restreints à aucun ensemble (d'après la définition, p. 161 de la conséquence ensembliste).

(iii) Mais la « simplicité » de $\overline{D}$ s'exprime beaucoup mieux à l'aide des notions de base de la Partie B : avec le bref exposé de ces notions (B, § 0), on reconnaît aisément que $\overline{Dem}$ est une règle de déduction *combinatoire* (« purement formelle »). Et il en résulte que si $A \in \overline{D}$, cela se vérifie d'une façon combinatoire.

(iv) Les lemmes 4 et 5 démontrent que $\mathscr{A}^*$ a pour conséquence : $E^{\mathscr{A}^*} \rightarrow D_1$.

Comme D_1 n'est pas conséquence de $\mathscr{A}^*$, le théorème 4 est ainsi démontré.

[LEMME 3. — $\overline{V(x)} = \overline{D(x)}$, où D est $\mathsf{V}y\ Dem\ (y, x)$, et, $\overline{Dem}$ est la relation entre objets syntaxiques :

$$\bar{y} = (B, A_1, A_2), \bar{x} = A :$$

B est conjonction d'un sous-ensemble fini de $\mathscr{A}^*$.
A_2 est la forme prénexe de $B \rightarrow A$ (définie Chap. 2, p. 17).
A_1 est une tautologie de la forme :

$$F(t_1^1, ..., t_m^1) \vee \cdots \vee F(t_1^k, ..., t_m^k)$$

telle que $\mathsf{V}x_1 \ldots \mathsf{V}x_m\, F(x_1, ..., x_m)$ soit $\check{A}_2$ (définie Chap. 2, p. 20) et $t_1^1 \ldots t_m^k$ soient des termes construits sur les symboles fonctionnels de $F(x_1, ..., x_m)$.

Démonstration. — Par le théorème de finitude, si A est conséquence de $\mathscr{A}^*$, il l'est d'un sous-ensemble fini B. $B \rightarrow A$ est valide. Appliquer alors Chap. 2, p. 21.

Remarques. — Si V est la définition du Chap. 2 de validité dans tous les modèles de $\mathscr{A}^*$ la simplification du lemme 3 est la suivante : pour vérifier qu'une formule est dans $\overline{V}$ on aurait à « examiner » *toutes* les réalisations de $\mathscr{A}^*$; pour vérifier qu'elle est dans $\overline{D}$, il faut simplement examiner toutes les configurations finies (B, A_1, A_2), et vérifier si la condition $\overline{Dem}$ est satisfaite ; si A est dans $\overline{D}$, cela se vérifie en un nombre fini d'essais (cf. Chap. 2, p. 22).

LEMME 4. — *Pour toute A de $\mathscr{L}_E$.*

$$\mathscr{A}^* \vdash D(\ulcorner A \urcorner) \to D(\ulcorner D(\ulcorner A \urcorner)\urcorner) .$$

Avant de décrire la démonstration, remarquons que $A \to D(\ulcorner A \urcorner)$ n'est pas vrai pour toute formule close A : pas si A est vraie, mais A n'est pas conséquence de $\mathscr{A}^*$! (par exemple pour $A = V_1$). Donc le lemme 4 repose sur les propriétés de la formule $D(\ulcorner A \urcorner)$, lesquelles reposent sur la remarque ci-dessus. Pour un choix canonique de Dem, en fait pour le choix le plus naturel, et pour une définition canonique des suites de symboles de $\mathscr{L}_E$, $\overline{Dem}\big((b, a_1, a_2), a\big)$ implique :

la formule $\vee x \vee y[C_{\bar{a}}(x) \wedge C_{(\bar{b}, \bar{a}_1, \bar{a}_2)}(y) \wedge Dem(y, x)]$ peut être formellement démontrée à partir de $\mathscr{A}^*$.

On accepte implicitement cette assertion si l'on admet que le système formel $\mathscr{A}^*$ suffit à une formalisation des mathématiques combinatoires élémentaires vu que la vérification de $\overline{Dem}\big((b, a_1, a_2), a\big)$ est une suite finie de vérifications purement combinatoires.

Ensuite, si

$$\vee x \vee y[C_{\bar{a}}(x) \wedge C_{(\bar{b}, \bar{a}_1, \bar{a}_2)}(y) \wedge Dem(y, x)]$$

est conséquence de $\mathscr{A}^*$, il en est de même de :

$$\vee x[C_{\bar{a}}(x) \wedge \vee y\, Dem(y, x)] .$$

La dernière étape est de montrer que la déduction esquissée ci-dessus peut être elle-même formalisée dans $\mathscr{A}^*$.

On note d'abord que l'affirmation *avec variables* b, a_1, a_2 (pour un A donné) :

$$Dem\big((b, a_1, a_2), \ulcorner A \urcorner\big) \to \vee x \vee y[x = F_G(b, a_1, a_2) \wedge Dem(y, x)]$$

est conséquence de $\mathscr{A}^*$, où G est la formule $Dem\big((b, a_1, a_2), \ulcorner A \urcorner\big)$ et où F_G est définie p. 174. Par conséquent $\mathscr{A}^*$ implique

$$\vee x \vee y[x = F_G(b, a_1, a_2) \wedge Dem(y, x)] \to \vee x \vee y[C_{A'}(x) \wedge Dem(y, x)] ,$$

où $A' = \vee y\, Dem(y, \ulcorner A \urcorner)$, i. e., $D(\ulcorner A \urcorner)$, et donc

$$Dem\big((b, a_1, a_2), \ulcorner A \urcorner\big) \to D(\ulcorner D(\ulcorner A \urcorner)\urcorner) .$$

Puisque les variables b, a_1, a_2 ne figurent pas dans la conclusion, il en résulte que

$$D(\ulcorner A \urcorner) \to D(\ulcorner D(\ulcorner A \urcorner)\urcorner)$$

est conséquence de $\mathscr{A}^*$.

La démonstration détaillée fait intervenir les définitions canoniques pour les raisons qu'explicite la remarque (iii).

LEMME 5. — *Supposons D choisie canonique, donc satisfaisant aux conditions : le lemme* 4 *est vérifié et (pour tout couple de formules A, B de* $\mathscr{L}_E$)

(1) $\mathscr{A}^* \vdash A \leftrightarrow B$ entraîne $\mathscr{A}^* \vdash D(\ulcorner A \urcorner) \leftrightarrow D(\ulcorner B \urcorner)$.
Alors si D_1 *est la formule déduite de D dans le lemme* 1,

$$\mathscr{A}^* \vdash E^{\mathscr{A}^*} \to D_1$$

a) Tout modèle de $\mathscr{A}^*$, s'il en existe, qui satisfait une formule close A, ne satisfait pas $\neg A$, et il en résulte trivialement :

$$[E^{\mathscr{A}^*} \wedge V(\ulcorner A \urcorner)] \to \neg V(\ulcorner \neg A \urcorner) .$$

Ce résultat élémentaire est conséquence de $\mathscr{A}^*$, cf. p. 172 (ii). La condition $E^{\mathscr{A}^*}$ est ici nécessaire car s'il n'existe aucun modèle de $\mathscr{A}^*$, $V(\ulcorner B \urcorner)$ est trivialement satisfait pour tout B, en particulier $B = \neg A$.

b) La démonstration de $D \to V$ (Lemme 3) est formalisable : $\mathscr{A}^* \vdash D \to V$ (sinon on appliquerait la remarque p. 172 (ii)).

En particulier, pour toute formule A de $\mathscr{L}_E$,

$$\mathscr{A}^* \vdash D(\ulcorner A \urcorner) \to V(\ulcorner A \urcorner)$$

et donc

$$\mathscr{A}^* \vdash \neg V(\ulcorner \neg A \urcorner) \to \neg D(\ulcorner \neg A \urcorner) ,$$

d'où, par application de *a*)

(2) $$\mathscr{A}^* \vdash [E^{\mathscr{A}^*} \wedge D(\ulcorner A \urcorner)] \to \neg D(\ulcorner \neg A \urcorner) .$$

c) Prenant $A = D_1$ dans (2)

$$\mathscr{A}^* \vdash [E^{\mathscr{A}^*} \wedge D(\ulcorner D_1 \urcorner)] \to \neg D(\ulcorner \neg D_1 \urcorner) ,$$

et prenant $A = \neg D_1$, $B = D(\ulcorner D_1 \urcorner)$ dans (1), puisque d'après le lemme 1, $\mathscr{A}^* \vdash D(\ulcorner D_1 \urcorner) \leftrightarrow \neg D_1$,

$$\mathscr{A}^* \vdash \neg D(\ulcorner \neg D_1 \urcorner) \leftrightarrow \neg D(\ulcorner D(\ulcorner D_1 \urcorner)\urcorner) .$$

Donc

$$\mathscr{A}^* \vdash [E^{\mathscr{A}^*} \wedge D(\ulcorner D_1 \urcorner)] \to \neg D(\ulcorner D(\ulcorner D_1 \urcorner)\urcorner) .$$

Ceci contredit le lemme 4 appliqué à $A = D_1$.

Donc $\mathscr{A}^* \vdash E^{\mathscr{A}^*} \rightarrow \neg D(\ulcorner D_1 \urcorner)$, c'est-à-dire

$$\mathscr{A}^* \vdash E^{\mathscr{A}^*} \rightarrow D_1 .$$

Discussion du théorème 4.

1. [$\mathscr{A}$ faillit, et donc] $\mathscr{A}^*$ faillit à caractériser la s. c. t., au sens du § 1, parce que [$U^{\mathscr{A}}$, n'est pas satisfait, donc] $U^{\mathscr{A}^*}$ n'est pas satisfait.

2. En plus $D^{\mathscr{A}^*}[D^{\mathscr{A}}]$ n'est pas satisfait par rapport aux raisonnements intuitifs sur les ensembles de type assez grand, voir théorème 3.

3. Par rapport aux raisonnements intuitifs concernant les ensembles finis, $D^{\mathscr{A}^*}$ n'est pas satisfait parce que $\mathscr{A}^*$ ne décide pas D_1, qui est une propriété combinatoire. En effet, $\overline{D(x)}$ est une propriété combinatoire, cf. (iii), p. 176 et, la construction de S étant combinatoire, D_1 l'est (cf. Lemme 1).

[Il faut signaler une différence importante entre le théorème 4 et les théorèmes d'indépendances mieux connus, par exemple en géométrie : l'indépendance de $E^{\mathscr{A}^*}$ est liée de façon essentielle au remplacement de l'axiome 3 par le schéma 3* ; en effet, $E^{\mathscr{A}^*}$ est conséquence de $\mathscr{A}$ (cf. th. 1) alors que, par exemple, l'axiome des parallèles est indépendant des autres axiomes de la géométrie qu'ils soient formulés au premier ou au second ordre. Considérez les axiomes de Pasch ou de Hilbert, formulés dans le langage suivant : variables de « points » ; relation $C(a, b, c, d)$: le segment ab est congruent au segment cd ; relation « a, b, c, colinéaires » ; relation « a entre b et c », etc... Tous les axiomes sont du premier ordre, sauf « l'axiome de continuité », i. e. l'axiome des coupures de Dedekind. Quelquefois cet axiome est remplacé par un schéma du premier ordre, qui ne considère que les coupures définies par des formules du langage ci-dessus. Mais l'axiome des parallèles est indépendant de l'axiome de continuité du second ordre et non pas seulement du schéma du premier ordre.]

4. D'après le corollaire 1, $X^{\mathscr{A}_F}$ n'est jamais vérifié parce que $\mathscr{L}_E$ n'utilise que des formules finies : l'ensemble t du corollaire 1 est défini par :

$$(x = \ulcorner A_1 \urcorner \wedge A_1) \vee (x = \ulcorner A_2 \urcorner \wedge A_2) \vee \cdots$$

où $A_1, A_2, \ldots$ est une énumération des formules closes de $\mathscr{L}_E$.

5. A l'encontre de ces résultats négatifs, il y a le corollaire positif des théorèmes 3 et 4 :

Une assertion purement combinatoire, D_1, indépendante de $\mathscr{A}^*$, est conséquence de $\mathscr{A} \cup \{ I_2 \}$ i. e. d'un « axiome d'infini » supplémentaire (axiome exprimant l'existence d'ensembles de type élevé).

D'un point de vue naïf, les inadéquations 1-4 ne sont pas surprenantes, justement parce que l'adéquation des axiomes du § 1 aux structures classiques

l'était. De l'oubli de cette surprise originelle vient l'étonnement suscité par le théorème de Gödel. Ce résultat semble proche des cas suivants bien connus :

(i) L'irrationalité de $\sqrt{2}$ a montré que les rationnels étaient inadéquats à la géométrie euclidienne, et non que celle-ci devait être rejetée ;

(ii)

$$2^{\aleph_0} \times 2^{\aleph_0} = 2^{\aleph_0}$$

a montré que la notion de bijection était inadéquate pour l'analyse du concept de dimension, et non que ce concept était dépourvu de sens mathématique.

Au § 4*c*) est discutée une opinion qui tire des conclusions tout à fait différentes du théorème 4. Mais d'abord on examine la valeur des concepts ensemblistes en considérant leurs possibilités de développement.

3. Progrès de la théorie. Acceptant toujours la s. c. t. nous allons considérer deux directions de recherches :

a) *l'addition*, et *b*) *l'élimination d'axiomes.*

a) Etudiant s. c. t., on peut suivre les méthodes mathématiques usuelles pour les structures particulières (entiers, réels, etc.), où « tous les moyens sont bons » si mathématiquement exacts. De ce point de vue la formulation d'axiomes, au § 2*c*), n'est qu'un commencement, et l'analyse qui a conduit à les poser doit se poursuivre. Les résultats du § 2*d*) montrent qu'il y a quelque chose à faire même si l'on se borne à des questions formulées dans le langage $\mathscr{L}_E$, vu que toutes les assertions ne sont pas décidées par $\mathscr{A}^*$ [$\mathscr{A}$] :

(i) Le théorème 2 réclame l'addition d'axiomes d'infini, i. e. d'axiomes exprimant l'existence d'ensembles de type élevé ; l'un d'eux est l'axiome de remplacement qui, par exemple, implique que pour tout bon ordre il existe un ensemble de *type* isomorphe à cet ordre.

$$[\bigwedge X \bigwedge a \{ (\bigwedge x \in a) \bigvee ! y X(x, y) \}] \to \bigvee z \bigwedge u \{ u \in z \leftrightarrow \bigvee x [x \in a \wedge X(x, u)] \}.$$

Les problèmes généraux que pose la formulation de tels axiomes sont discutés dans : K. Gödel, What is Cantor's continuum problem, *Amer. Math. Monthly*, **54** (1947), 515-525.

(ii) Un défaut particulier de [systèmes du premier ordre comme] $\mathscr{A}^*$, est que $C_{\alpha+1}$ est censé comprendre *tous* les sous-ensembles de C_α, alors que 3* exprime seulement l'existence des sous-ensembles définissables par une formule de $\mathscr{L}_E$. En particulier rien n'est dit sur le sous-ensemble de C_ω, t, du corollaire 1 ci-dessus. [On notera que t est la réalisation d'une formule infinie ; c'est-à-dire que t est construit par une itération transfinie des opérations ensemblistes de base.

Une analyse conceptuelle systématique de ce genre de constructions intuitives réclamerait peut-être l'introduction de nouvelles notions primitives — pour ce

qui est de son intérêt, voir en p. 183 ce qu'apporte, du point de vue des fondements, l'analyse de la notion intuitive Val, résumée dans le théorème 5.]

Un examen approfondi suggère que le défaut (i) est plus fondamental que (ii) : (ii) concerne seulement l'opération *de base* (de formation) de l'ensemble des parties d'un ensemble, tandis que (i) concerne le nombre d'*itérations* de cette construction, une matière dont la théorie est bien plus difficile. [Plus formellement, dans (i) on s'efforce de répondre à l'inadéquation de systèmes d'axiomes du premier *et* du second ordre, dans (ii) seulement à celle de systèmes du premier ordre. Et de toutes façons (pour la définition du Chap. 7 de conséquence du second ordre), toute assertion de la forme :

« *la formule A est conséquence du second ordre de B* »

s'exprime dans le langage du premier ordre $\mathscr{L}_E$ (s. c. t. étant sa réalisation) : donc la justification d'une telle assertion revient à la formulation d'axiomes (éventuellement indépendants des systèmes actuels) de $\mathscr{L}_E$, qui relève de (i).

On notera une propriété analogue de l'inadéquation de $\mathscr{L}_E$ vis-à-vis des notions de la s. c. t. qui s'expriment naturellement par des formules infinies, comme t : au moins pour des formules à quantificateurs bornés, la réalisation $\bar{A}$ d'une formule infinie A peut être définie par une expression de $\mathscr{L}_E$. Néanmoins, d'un point de vue heuristique, il peut être essentiel de conserver aux assertions sur s. c. t. la forme de formules infinies ou du second ordre].

Pour plus d'information sur les relations entre (i) et (ii), consulter : GÖDEL, Remarks before the Princeton Bicentennial Conference on problems in mathematics, pp. 84-88 de : *The Undecidable*, ed. Martin Davis, N. Y. 1965).

Remarque sur les axiomes d'infini et les mathématiques traditionnelles.

Les axiomes d'infini sont intéressants, non seulement en eux-mêmes, mais aussi de par la possibilité de les utiliser pour la démonstration de propriétés des ensembles de type bas ; ainsi par exemple l'axiome I_2 sert à prouver $E^{\mathscr{A}^*}$, donc l'assertion D_1, qui est purement arithmétique (i. e. : assertion formulée dans $\mathscr{L}_E$, dont tous les quantificateurs sont restreints à $\langle C_\omega, \in_\omega \rangle$).

Bien entendu, la *vérité* de D_1 ne « dépend » pas de l'existence de $\langle C_{\omega+\omega+1}, \in_{\omega+\omega+1} \rangle$, mais son *évidence* par contre en dépend ! Cet usage de I_2 est parallèle à celui de méthodes analytiques en théorie des nombres, où les propriétés des fonctions de variables complexes (qui sont des éléments de $\langle C_{\omega+2}, \in_{\omega+2} \rangle$) ont des conséquences arithmétiques. Mais il faut noter deux différences. Premièrement, comme il sera discuté en détail en B, p. 197, l'usage des fonctions de variables complexes peut être éliminé dans toutes les démons-

trations *connues* de théorie analytique des nombres, en ce sens (logique) précis que les théorèmes connus sont également conséquences de $\mathscr{A}^*_-$ (cf. § 2*d*). (En pratique les déductions à partir de $\mathscr{A}^*_-$ sont plus difficiles à suivre, parce que les fonctions complexes doivent être remplacées par des approximations rationnelles explicitement définies.) Par contre D_1 n'est pas une conséquence de $\mathscr{A}^*$, ni à fortiori de $\mathscr{A}^*_-$. Deuxièmement en termes informels, D_1 a surtout un « intérêt » *métamathématique* et non arithmétique. Plus précisément on ne sait pas si certains problèmes ouverts *familiers* en théorie des nombres sont décidés par des axiomes de l'infini.

b) En ce qui concerne l'*élimination* d'axiomes (de $\mathscr{A}^*$) : son intérêt pour la théorie des fondements ensemblistes n'est pas très différent, en principe, de l'intérêt pour les études axiomatiques ordinaires. Ainsi, dans la pratique mathématique, l'ensemble réduit d'axiomes devrait être satisfait par une structure mathématique importante ne satisfaisant pas aux axiomes originels. Donc ici, si $\mathscr{A}^*$ était réduit à un sous-ensemble $\mathscr{A}_1$, on souhaiterait que $\mathscr{A}_1$ soit satisfait par un concept important d'ensemble qui ne satisfasse pas $\mathscr{A}$; mais pour être important *en théorie des fondements*, ce concept devrait être fondamental, donc évidemment non défini en termes de s. c. t. : au contraire, d'après le critère du § 2*a*) pour les fondements « réalistes », la s. c. t. devrait être définissable à partir de ce nouveau concept (4).

Aucun concept fondamental de cette sorte n'est connu à présent. (La notion générale de propriété, i. e. d'ensemble au sens (iii) du § 2*a*), a été mentionnée comme notion de base possible pour les fondements, mais sa logique n'est pas suffisamment étudiée pour être discutée ici.)

> N. B. On verra ci-dessous que la possibilité d'éliminer systématiquement certains axiomes de $\mathscr{A}^*$ des démonstrations connues à présent dans certaines parties de la pratique mathématique est importante pour les fondements (non ensemblistes) des mathématiques décrits en B.

[4. Notes historiques et compléments sur la validité logique.

Un langage $\mathscr{L}$ du calcul des prédicats est donné, comportant un nombre fini de symboles de relations et de fonctions ; Val^1, Val^2, ... désignent les ensembles des formules de $\mathscr{L}$, $\mathscr{L}^2$, ... qui sont intuitivement valides, $\overline{V}^1$, $\overline{V}^2$, ... ceux des formules valides au sens des Chapitres 2 et 7.

---

(4) De même que les règles de déduction (cf. note 3), les axiomes de la théorie des ensembles qui interviennent dans les déductions sont rarement mentionnés dans la pratique, et rares sont les tentatives pour éviter l'emploi d'axiomes formellement non nécessaires, ce qui contraste avec les efforts déployés pour éliminer les hypothèses superflues dans les théorèmes d'algèbre ou de topologie. Cette pratique est tout à fait cohérente si l'on admet la compréhension tacite de quelque chose comme les ensembles de la s. c. t., et si aucune autre notion de base indépendante n'est connue. Elle serait complètement anti-scientifique si l'on s'intéressait sérieusement à une justification « empirique » des axiomes : car si, dans la pratique, tous les raisonnements n'employaient qu'un sous-ensemble $\mathscr{A}_1$ de $\mathscr{A}^*$, l'expérience justifierait au mieux $\mathscr{A}_1$!

a) *Quelques résultats ensemblistes* (i. e. formulés dans $\mathscr{L}_E$, avec comme toujours la s. c. t. pour réalisation) *qui servent à établir des relations entre les notions ensemblistes* $\overline{V}^i$ *et les notions intuitives primitives* Val^i.

$\overline{Dem}_0$ (cf. p. 176) désigne la relation :
$\{ \langle A_1, A \rangle : A$ est une formule prénexe de $\mathscr{L}$, $\check{A}$ est $\mathsf{V}x_1 \ldots \mathsf{V}x_m\, F$ et A_1 est une identité propositionnelle de la forme

$$F(t_1^1, \ldots, t_m^1) \vee \cdots \vee F(t_1^n, \ldots, t_m^n)\} .$$

On pose $$D_0 = \mathsf{V}y\, Dem_0.$$

(I) $\overline{V}^1 \subset \overline{D}_0$. Ce résultat ensembliste est démontré au Chapitre 2 comme l'est, p. 160, la complétude de D pour $\overline{V}$.

De la note 3, p. 176 découlent deux propriétés des notions intuitives de validité logique :

(II) $\mathrm{Val}^i \subset \overline{V}^i$ et (III) $\overline{D}_0 \subset \mathrm{Val}^1$.

Théorème 5. — $\mathrm{Val}^1 = \overline{D}_0 = \overline{V}^1$.
(Conséquence immédiate de I, II, III.)

Corollaire 5. — $\overline{D}_0 \subset \overline{V}^1$ *résulte de* II *et* III *sans utilisation du théorème p.* 21 *du Chapitre* 2.

> N. B. $\overline{D}_0 \subset \overline{V}^1$ est donc un résultat purement ensembliste démontré à l'aide de la notion primitive Val^1. Cet usage de Val^1 n'est pas nécessaire parce que la démonstration p. 121 peut être formalisée dans $\mathscr{A}_-^*$ par exemple (cf rem. (ii), p. 171) ; autrement dit, la condition $D^{\mathscr{A}^*}$ du § 1 est satisfaite au moins vis-à-vis de cette démonstration particulière utilisant Val^1. Cependant on pourrait peut-être dériver de nouveaux axiomes pour s. c. t. en utilisant de manière semblable des notions logiques intuitives.

Historiquement, les premières règles formelles de validité logique des formules du premier ordre (quelque peu différentes de $\overline{\mathrm{Dem}}_0$), ont été énoncées par Frege ; pour ces règles, les propriétés (correspondant à) II et III étaient aussi évidentes. Cependant (ce qui correspondait à) $\mathrm{Val}^1 \subset \overline{D}_0$ était seulement soupçonné, et ne fut prouvé que 50 ans plus tard environ, par Gödel.

Sur la possibilité d'étendre le théorème 5 aux formules d'ordre supérieur : on ne dispose pas présentement d'une démonstration convaincante de $\mathrm{Val}^2 = \overline{V}^2$; et l'alinéa suivant montrera qu'une extension de $\overline{D}_0 = \overline{V}^1$, même sous certaines formes plus faibles, est impossible. Pour voir que ceci n'affecte pas la clarté de la notion Val^2, il y a lieu de comparer nos raisons actuelles d'admettre $\mathrm{Val}^2 = \overline{V}^2$, et celles qu'on avait, *avant* la démonstration de Gödel, d'admettre $\mathrm{Val}^1 = \overline{V}^1$.

D'abord, chaque fois que la pratique actuelle montre l'appartenance à $\overline{V}^i$

d'une formule (*aussi bien* pour $i = 1$ et $i = 2$), elle peut montrer son appartenance à Val^i ; et inversement. Ensuite, pour beaucoup de $A \in \mathscr{L}^2$ on ignore si $A \in \overline{V}^2$ ou non ; mais *aussi bien* il n'y a pas de méthode effective pour décider, pour A dans $\mathscr{L}$ arbitraire, si $A \in \overline{V}^1$ ou non (et ce, *même en disposant* du Théorème 5).

b) *Compléments sur* $\overline{V}^1$ *et* $\overline{V}^2$: les exercices 1 et 7 du Chapitre 7 montrent que le théorème de finitude n'est pas vrai pour la conséquence du second ordre, ni même pour des formules infinies du premier ordre (bien qu'une extension en soit connue dans ce dernier cas, cf. le résumé du Chap. 6).

On peut formuler des résultats plus détaillés en utilisant la notion de validité dans $\langle C_\alpha, \in_\alpha \rangle$: V_α^i désigne l'ensemble des formules de $\mathscr{L}^i$, vraies dans toutes les réalisations de $\mathscr{L}^i$ qui appartiennent à C_α. Evidemment $V_\alpha^i \supset V_\beta^i$ si $\alpha < \beta$.

(i) $\alpha > \omega$ entraîne $\overline{V}^1 = V_\alpha^1$ (Chap. 2, Ex. 5).

(i′) Sauf pour des langages très pauvres, $V_\omega^1 \neq V_{\omega+1}^1$ (la formule qui traduit : « tout ordre total a un plus petit élément », appartient à V_ω^1, non à $V_{\omega+1}^1$).

(ii) Par exemple pour $\mathscr{L} = \mathscr{L}_E$, $V_{\omega+\omega+1}^2 \neq V_{\omega+\omega}^2$ car $\mathscr{A}$ admet un modèle dans $\langle C_{\omega+\omega+1}, \in_{\omega+\omega+1} \rangle$, non dans $\langle C_{\omega+\omega}, \in_{\omega+\omega} \rangle$. Plus généralement, pour $I \in \mathscr{L}_E^2$ (I étant par exemple un axiome d'infini), si α_I est tel que $\mathscr{A} \cup \{I\}$ a un modèle dans C_{α_I+1}, mais pas dans C_{α_I}

$$V_{\alpha_I+1}^2 \neq V_{\alpha_I}^2 .$$

Visiblement il existe une borne supérieure α_E pour ces α_I, à savoir la borne de : $\{\alpha_I ; I \in \mathscr{L}_E^2$ et α_I est le plus petit α tel que $I \notin V_\alpha^2$ si $I \notin V^2$, $\alpha_I = 0$ si $I \in V^2\}$. Mais on sait peu de choses sur la grandeur de α_E.

Pour discuter l'existence d'une formule D^2 jouant vis-à-vis de $\overline{V}^2$ un rôle analogue à celui de D_0 vis-à-vis de $\overline{V}^1$, rappelons une propriété essentielle pour le caractère « élémentaire » de D_0 : tous les quantificateurs de D_0 sont restreints à $\langle C_\omega, \in_\omega \rangle$, au contraire de V^1 d'après (i′). (Il y a d'autres propriétés dont l'analyse plus délicate relève de la partie B, mais elles n'interviennent pas dans le résultat négatif particulier qui suit.)

Comme au Chapitre 6, la phrase « restreint à $\langle C_\alpha, \in_\alpha \rangle$ » signifie que chaque quantificateur en x intervient sous la forme $\bigvee x(T_\alpha(x) \wedge \cdots)$ ou $\bigwedge x(T_\alpha(x) \rightarrow \ldots)$, où T_α est la formule canonique qui définit C_α (lorsque $\mathscr{L}_E$ est interprété par s. c. t.). La formule *canonique* T_α a de plus la propriété de définir C_α lorsque $\mathscr{L}_E$ est réalisé par $\langle C_\beta, \in_\beta \rangle$, pour tout $\beta \geqslant \alpha$ (comparez Chap. 5, Ex. 6 *c*).

Résultat négatif. Si α est tel que : il existe une formule A_α de $\mathscr{L}_E^2$ dont l'unique modèle, à un isomorphisme près, est $\langle C_\alpha, \in_\alpha \rangle$, alors $\overline{V}^2 \neq \overline{D}^2$, pour toute

formule D^2 de $\mathscr{L}_E$ dont les quantificateurs sont restreints à $\langle C_\alpha, \in_\alpha \rangle$. Ceci est une conséquence immédiate du Nota Bene du lemme 2, p. 175.

En d'autres termes : le lemme 2 montre que certains systèmes d'axiomes du second ordre ne sont pas saturés vis-à-vis de toutes les assertions de la forme $A \in V^2$ (A de $\mathscr{L}^2$), tandis que : moyennant l'hypothèse ci-dessus sur α, il y a des systèmes saturés vis-à-vis des formules closes dont les quantificateurs sont restreints à C_α. On dit que toutes *ces formules sont décidées au sens de la conséquence du second ordre*.

Remarquons que $\mathscr{A}$ lui-même décide toutes les formules de $\mathscr{L}_E$ dont les quantificateurs sont restreints à $C_{\omega+n}$ (défini canoniquement) pour tout entier n. Une formule de ce type est l'hypothèse du continu (CH) qui est restreinte à $C_{\omega+2}$: CH exprime que tout sous-ensemble de $C_{\omega+1}$ est en bijection soit avec $C_{\omega+1}$ soit avec un sous-ensemble de C_ω ; or de telles bijections sont éléments de $C_{\omega+2}$.

En résumé nous avons moins de renseignements sur $\overline{V}^2$ que sur $\overline{V}^1$, mais dans ce que nous avons dit, rien ne suggère que $\overline{V}^2$ soit moins bien *définie* que $\overline{V}^1$: en fait ce sont les *mêmes* notions ensemblistes qui servent dans chacune de ces définitions.

c) *Une position privilégiée pour les formules finies du premier ordre et la notion de conséquence du premier ordre* ? Nous avons décrit tous les résultats précédents en *acceptant* les notions primitives ensemblistes. De ce point de vue, les résultats au sujet de $\overline{V}^2$, V_α^2, montrent que $\overline{V}^2$ est compliquée, non qu'elle est imprécise. De même (cf. p. 180), le théorème 4 montre l'insuffisance de la conséquence du premier ordre pour analyser la s. c. t., non que la s. c. t. doive être rejetée.

Comme annoncé p. 180, nous exposons maintenant une position courante qui tire des conclusions différentes ; bien que la forme la plus pure de positivisme en théorie des fondements soit le formalisme grossier, qui sera examiné dans la Partie B, § 4, cette position est apparentée au positivisme, mais encore moins cohérente.

En gros, elle affirme que le théorème 4 (la non-saturation) n'établit pas du tout une *inadéquation* : les formules de $\mathscr{L}_E$ qui ne sont pas conséquences formelles du système d'axiome donné, disons $\mathscr{A}^*$, ne doivent pas être considérées comme vérités ensemblistes. Par conséquent cette position ne peut que rejeter les tentatives discutées au § 3 pour trouver de nouveaux axiomes.

La justification générale donnée est qu'il n'y a rien à découvrir parce que la notion d'ensemble est *définie* par le système d'axiomes choisi (ici $\mathscr{A}^*$), exactement comme la notion de groupe l'est par les axiomes de groupe.

Alors toute structure S satisfaisant les axiomes choisis doit être considérée comme structure ensembliste et il se trouve que ces structures ne sont pas toutes isomorphes.

Evidemment ceci suppose implicitement qu'on se confine aux systèmes d'axiomes du premier ordre (car il existe des axiomes du second ordre catégo-

riques). Donc elle ne peut que rejeter l'usage qui est fait aux § 3 et § 4*b*) de la notion de conséquence du second ordre. En particulier elle interpréterait ainsi les propriétés de décidabilité, comme par exemple

$$(+)\{(\mathscr{A} \rightarrow CH) \in V^2\} \vee \{(\mathscr{A} \rightarrow \neg CH) \in V^2\},$$

qui est la décidabilité de CH :

$(+)$ est un théorème ensembliste, c'est-à-dire, *d'après la position*, une conséquence des axiomes choisis $\mathscr{A}^*$; mais *chaque* structure ensembliste a sa *propre* relation de conséquence du second ordre (qui est la réalisation $\bar{V}_S^2$ de la formule canonique V^2), et $(+)$ exprime que dans S ou bien le premier membre, ou bien le second est vérifié. La position comparerait $(+)$ à la trivialité logique :

$$\wedge x \wedge y\,(x \circ y = y \circ x) \vee \neg \wedge x \wedge y\,(x \circ y = y \circ x),$$

satisfaite dans chaque groupe muni de la loi $\circ$; mais cela ne signifie pas que tous les groupes sont commutatifs ou tous non commutatifs !

Un défaut tout à fait évident de la comparaison avec les axiomes de groupe, est que ceux-ci ne sont pas censés, comme $\mathscr{A}^*$, exprimer les propriétés d'une structure particulière (privilégiée). Et certainement, rien de ce que nous savons du concept général de groupe n'exclut l'existence de groupes particuliers ! Voici encore deux objections :

1. La notion de modèle ou réalisation (d'axiomes donnés) est définie à l'aide des notions de base ensemblistes. En remplaçant la s. c. t. par le mot « structure » ou « objet mathématique » S, on ne fait que changer le problème du § 3 en problème de la découverte d'axiomes valides pour la notion de « structure ». Rien n'a été proposé pour une telle recherche.

2. Evidemment, si l'on n'accepte pas la notion de base s. c. t., la notion de conséquence du second ordre sera également relative (à S).

Cependant si la conséquence du second ordre est définie par $\bar{V}_s^2$ dans toute structure ensembliste S, pourquoi pas $\bar{V}^1$ ou $\bar{D}_0$? Le lemme 2, p. 175, montre qu'alors la notion de conséquence du premier ordre dépendrait également de S !

De façon tout à fait générale, cette position appelle les objections suivantes : elle est incohérente quand d'une part elle accepte la notion de structure abstraite (de modèle), et d'autre part rejette la considération de structures privilégiées : bien sûr, si un système d'axiomes du premier ordre possède un modèle infini il en possède beaucoup d'autres ; mais la seule justification que nous ayons pour supposer que, par exemple, $\mathscr{A}^*$ en possède *un* c'est justement la structure particulière $\langle C_{\omega+\omega}, \in_{\omega+\omega} \rangle$.

Ensuite, la restriction à la conséquence du premier ordre, visiblement empruntée aux fondements combinatoires (Partie B), est justifiée superficiellement. Dans les fondements combinatoires, elle est justifiée car elle permet d'éviter de façon cohérente les hypothèses sur des structures abstraites, en ne considérant que la définition de la conséquence du premier ordre par les règles

formelles $\overline{D}_0$. Pour la position présente, la justification est sans doute le théorème $\overline{V}^1 = \overline{D}_0$. Mais comme on considère des structures abstraites, (pour serrer de plus près la pratique mathématique), on ne voit pas l'avantage qu'elle tire du recours aux règles formelles.

De plus, $\overline{V}^1$, et donc le théorème $\overline{V}^1 = \overline{D}_0$, n'ont de sens que si l'on accepte des structures privilégiées (en particulier le Théorème cité suppose l'existence de structures infinies, voir § 4*b* (i')).

Cette position, en essayant de gagner sur tous les tableaux, ne réalise donc qu'une combinaison boîteuse des deux types de fondements ici décrits.

Il y a deux liens entre le positivisme et cette position. D'abord la restriction déjà mentionnée aux formules (finies) du premier ordre. Ensuite et surtout le fait que ni le positivisme ni cette position ne fournissent la moindre contribution positive aux fondements, et sont essentiellement une consolation de ce que certains problèmes de fondements ne se résolvent pas exactement comme on l'avait souhaité.]

B. FONDEMENTS COMBINATOIRES

Les notions de base sont celles de *mot* (suite finie de symboles) d'un alphabet fini, de *fonction combinatoire* (dont les arguments et les valeurs sont des mots), et de *preuve combinatoire* d'identités (entre deux fonctions combinatoires, par exemple $(a.a) - (b.b)$ et $(a + b).(a - b)$).

Ces notions sont supposées connues dans la théorie combinatoire des fondements, comme l'étaient les notions ensemblistes dans la Partie A et, d'ailleurs, dans tout le texte principal. Evidemment une analyse des notions de *base* ne cherche pas à les définir en terme d'*autres* notions ; cf. A, § 2*a* pour une analyse non formelle de la notion d'ensemble, analyse qui consiste, entre autre, en des distinctions non formelles.

Le lecteur découvrira que les notions combinatoires sont assez familières parce qu'elles interviennent implicitement dans toutes les mathématiques élémentaires (cf. § 0). Seule la formulation explicite de ses propres connaissances peut lui paraître originale.

Il ne s'agit ici que d'une esquisse de la théorie combinatoire parce qu'un exposé précis réclamerait la connaissance de la théorie des démonstrations, partie de la logique mathématique qui n'est pas traitée dans ce livre. Mais le lecteur doit, au moins, avoir regardé un système formel comme celui du chapitre I de Bourbaki.

La numérotation des parties A et B met en évidence la correspondance entre les deux théories de fondements considérées ici : en particulier, le § 1 formule les conditions d'adéquation (pour la théorie en question) et le § 2 énumère quelques propriétés utiles des notions de base. Le § 0 ci-dessous contient une esquisse des notions de langage combinatoire et de réalisation combinatoire, qui correspondent aux notions de langage, respectivement de réalisation, pour les fondements ensemblistes de la Partie A.

Avertissement. — Il faut distinguer les *preuves*, traitées ici, des dérivations formelles, c'est-à-dire des suites de formules obtenues en appliquant mécaniquement des règles formelles ; distinction analogue entre comprendre et copier une preuve mathématique. En particulier, partant d'une réalisation (combinatoire) d'un langage formel, une dérivation formelle *définit* ou *décrit* une preuve. Ceci correspond, dans l'analyse ensembliste, à la définition d'un ensemble par une formule (dont l'ensemble est sa réalisation au sens de la p. 160 ; la notion de formule du calcul des prédicats est telle que les relations syntaxiques

entre les parties d'une formule correspondent à des relations (ensemblistes) entre leurs réalisations respectives. Dans la théorie combinatoire on choisit aussi des règles formelles de façon que l'on puisse associer une preuve combinatoire à toute suite de formules construite selon ces règles, et que les relations syntaxiques entre les parties de la suite correspondent à des relations naturelles entre les preuves associées à ces parties.

La doctrine formaliste mentionnée dans l'introduction ou bien n'accepte pas comme légitime la distinction entre preuve et dérivation formelle (parce qu'elle n'accepte pas la notion de preuve) ou bien la considère comme insuffisamment précise pour les mathématiques. L'introduction a déjà critiqué quelques présomptions de cette doctrine ; on y reviendra brièvement dans le § 4 après avoir exposé les conséquences principales de cette distinction.

0. Raisonnement combinatoire. – Les objets dont s'occupe ce type de raisonnement, et dont d'ailleurs il tire son nom, sont les combinaisons finies d'objets concrets tels que les lettres de l'alphabet, les chiffres, les symboles d'un langage formel, etc. Une fonction combinatoire à n-variables est une règle mécanique *avec* une preuve combinatoire de son caractère fonctionnel, c'est-à-dire une preuve démontrant que, appliquée à n objets (pris parmi les combinaisons considérées), la règle détermine une valeur après un nombre fini d'essais ; plus précisément, on applique la règle à une description (d'un objet) qui, en général, n'est pas l'objet même. Enfin, pour être combinatoire, une preuve ne doit faire intervenir qu'un nombre fini de fonctions combinatoires et la succession de toutes les combinaisons finies possibles.

Le lecteur trouvera une analyse détaillée des règles mécaniques dans la théorie des fonctions récursives et une analyse partielle des preuves combinatoires par la suite. Mais il pourra se faire une idée générale de ces notions en réfléchissant sur un exemple typique : la fonction combinatoire de l'*addition* en Arithmétique numérique.

(i) *Les objets et leur description.* — L'alphabet de l'Arithmétique numérique contient deux symboles : le symbole d'individu 1 et le symbole fonctionnel S à une variable. Par conséquent, les termes (mots) sont 1, $S1$, $SS1$, ..., notés aussi $S^0 1$, $S^1 1$, $S^2 1$, respectivement.

Ce qui est typique ici est qu'on peut décider mécaniquement si oui ou non deux termes désignent le même objet. Cette décision ne fait intervenir qu'un nombre fini de *constatations* d'égalités, resp. d'inégalités d'objets concrets qui se présentent (cf. l'acte de reconnaître une lettre de l'alphabet). Ce qui n'est pas typique est que tout objet considéré ici *est* un terme, tandis que, en général, un objet est *muni* d'un terme que l'on nomme sa description canonique et qui reflète les étapes de construction de l'objet. On notera que toutes les descriptions admises dans le raisonnement combinatoire permettent de retrouver mécaniquement les descriptions canoniques correspondantes, ce qui réduit à posteriori l'importance des descriptions canoniques d'objets (en contraste avec les descriptions de fonctions : voir *a*)).

N. B. Cette dernière remarque entraîne que, tant que l'on se confine aux *objets*, la théorie combinatoire approche l'analyse ensembliste : celle-ci, étant une théorie réaliste, supprime, *en principe*, tout appel aux descriptions des objets considérés (ensembles de l'échelle des types), principe qui conduit à l'axiome d'extensionnalité de A § 2. Par contre, ce principe n'est pas satisfait dans les mathématiques constructives au sens large (§ 3, ci-dessous) qui admettent aussi comme objets les fonctions et même les preuves constructives.

La pratique mathématique combinatoire prend les constatations d'égalité mentionnées comme données sans les analyser. En revanche, l'intérêt du raisonnement combinatoire pour la théorie de la connaissance est nettement lié au caractère élémentaire de ces constatations : celles-ci sont du même genre que les perceptions les plus simples, les objets considérés étant conçus comme des configurations finies existant dans l'espace et le temps. Ainsi les êtres abstraits n'entrent ici que dans les preuves : ils ne sont pas à leur tour des sujets d'un raisonnement combinatoire. (Les preuves en tant que pensées ne sont évidemment pas des configurations finies d'objets concrets ; en particulier, on verra qu'elles font intervenir l'idée de la succession *infinie* des combinaisons finies).

Sur le plan formel, la restriction ci-dessous aux langages ne contenant que = comme symbole relationnel, reflète le rôle central des constatations d'égalité.

(ii) *Les règles mécaniques et leur description.* — On augmente l'alphabet de (i) en ajoutant le symbole fonctionnel + à deux variables (et on écrira $t + t'$ pour $+ \, t \, t'$). Partant des formules

(*) $$a + 1 = Sa \qquad \text{et} \qquad a + Sb = S(a + b)$$

on substitue des termes aux lettres a et b, et on applique les règles dites d'égalité ; c'est-à-dire si on a « déduit » les équations $t_1 = t_2$ et $t' = t''$ on remplace dans $t' = t''$ une ou plusieurs parties de la forme t_1 par t_2.

N. B. Les formules (*) définissent ou décrivent la règle d'addition pourvu qu'on comprenne l'opération syntaxique de substitution et, en particulier, qu'on sache identifier des symboles identiques. En terme de machines à calculer le (*) correspond aux instructions sur la bande, et l'espèce de compréhension requise correspond au mécanisme de la machine préparée à réagir à ces instructions.

Des règles (ou, plutôt, définitions) non mécaniques de fonctions mathématiques abondent en Analyse, ce qui constitue d'ailleurs une différence essentielle entre les mathématiques étudiées à l'Université et celles étudiées au Lycée.

Par exemple, si $r_1, r_2, ...$ est une suite ρ de rationnels, disons entre 0 et 1, on définit une suite $A_0, A_1, ...$ d'intervalles qui convergent vers la borne inférieure de ρ par la « règle » suivante : $A_0 = [0, 1]$, A_{n+1} est la moitié gauche de A_n si A_n contient un élément de ρ, et, sinon, A_{n+1} est la moitié droite. En général, on ne sait pas quel terme de l'alternative est vrai. La théorie des fonctions récursives établit que beaucoup des définitions courantes en Analyse n'équivalent à aucune fonction définissable par une règle mécanique : à plus forte raison elles n'équivalent à aucune fonction combinatoire. (Cette conclusion ne réclame donc aucune analyse de la notion de preuve combinatoire, ces définitions étant « grossièrement » non constructives : en contraste avec les problèmes principaux du § 3 ci-dessous).

(iii) *Fonctions combinatoires.* — Pour compléter la règle mécanique de (ii) de façon à obtenir une fonction combinatoire on établit, à l'aide d'une preuve combinatoire que quels que soient les entiers $\boldsymbol{n}$ et $\boldsymbol{m}$, la règle permet de déduire une formule de la forme $S^{\boldsymbol{n}} 1 + S^{\boldsymbol{m}} 1 = S^{\boldsymbol{p}} 1$. Au m-ième élément de la suite $S^0 1, S^1 1, S^2 1, ...$ on fait correspondre une application de la règle (*) (pour un $\boldsymbol{n}$ donné) : si $\boldsymbol{m} = \boldsymbol{0}$, on déduit $S^{\boldsymbol{n}} 1 + S^{\boldsymbol{m}} 1 = S^{\boldsymbol{n}+1} 1$ en remplaçant a par $S^{\boldsymbol{n}} 1$ dans la première formule de (*) ; si $\boldsymbol{m} \neq \boldsymbol{0}$, on substitue $S^{\boldsymbol{m}-1} 1$ à b dans la deuxième formule de (*) ce qui donne

$$S^{\boldsymbol{n}} 1 + S^{\boldsymbol{m}} 1 = S(S^{\boldsymbol{n}} 1 + S^{\boldsymbol{m}-1} 1) .$$

Il reste à vérifier que les règles (particulières) d'égalité de (ii) suffisent pour en tirer la valeur cherchée : on raisonne par récurrence sur $\boldsymbol{m}$, c'est-à-dire on suit la construction de la suite $S^0 1, S^1 1, ..., S^{\boldsymbol{m}} 1$; partant d'une formule de la forme $S^{\boldsymbol{n}} 1 + S^{\boldsymbol{m}-1} 1 = S^{\boldsymbol{q}} 1$, on obtient $S^{\boldsymbol{n}} 1 + S^{\boldsymbol{m}} 1 = S^{\boldsymbol{q}+1} 1$ en prenant $S^{\boldsymbol{n}} 1 + S^{\boldsymbol{m}-1} 1$ pour t_1, $S^{\boldsymbol{q}+1}$ pour t_2, $S^{\boldsymbol{n}} 1 + S^{\boldsymbol{m}} 1$ pout t' et $S(S^{\boldsymbol{n}} 1 + S^{\boldsymbol{m}-1} 1)$ pour t''.

D'une façon semblable on vérifie l'unicité de p, m et n étant fixés. Bref, (la règle définie par) le terme $a + b$ est fonctionnel(le) sur l'alphabet de (i) parce que, quels que soient les entiers $\boldsymbol{n}$ et $\boldsymbol{m}$, une formule (unique) de la forme $S^{\boldsymbol{n}} 1 + S^{\boldsymbol{m}} 1 = S^{\boldsymbol{p}} 1$ est dérivable.

Plus généralement, on voit le caractère fonctionnel de la règle définie, au sens du (ii), par un terme de l'alphabet dont les variables sont $a, b, ..., c$, dont l'unique symbole d'individu est 1 et dont les symboles fonctionnels sont S et $+$.

N. B. L'espèce de compréhension requise pour appliquer une règle mécanique ne suffit évidemment pas pour suivre le raisonnement ci-dessus ; sur le plan formel la différence correspond à la différence syntaxique entre les formules sans ou avec variables.

Les explications qu'on a données dans (i), jointes aux connaissances intuitives du lecteur, lui permettent de reconnaître aisément le caractère combinatoire de la règle d'addition. Il est plus difficile de formuler explicitement ce qui est essentiel ici ; autrement dit, de formuler en

toute généralité les principes, c'est-à-dire les possibilités de l'imagination combinatoire, implicitement présupposés dans la preuve du caractère fonctionnel de la règle d'addition. (La formulation cherchée permettrait, en outre, une énumération, bien entendu non combinatoire, de toutes les fonctions combinatoires : voir § 3).

(iv) *Preuves d'identités et leurs relations aux dérivations formelles*. Soit $\mathscr{R}^+$ le système des règles obtenu en ajoutant à l'alphabet de (ii) des variables $a, b, ..., c$, et en étendant les règles de (ii) à toutes les équations construites sur l'alphabet augmenté. Soit $t_{(n,\ m,\ ...,\ p)}$ le terme obtenu en substituant $S^n\,1$, $S^m\,1, ..., S^p\,1$ à $a, b, ...,$ resp. c dans t, et, enfin, soit $\bar{t}$ la fonction combinatoire définie par le terme t au sens de (iii).

Une preuve combinatoire de (l'identité) $\bar{t} = \bar{t}'$ démontre, par définition, que quels que soient les entiers $\boldsymbol{n}, \boldsymbol{m}, ..., \boldsymbol{p}$ la formule $t_{(n,m,...,p)} = t'_{(n,m,...p)}$ peut être dérivée selon les règles de (ii).

α) On note d'abord qu'on peut obtenir une preuve de $\bar{t} = \bar{t}'$ à partir d'une dérivation formelle, selon les règles de $\mathscr{R}^+$, de la formule $t = t'$, $\mathfrak{R}^+$ étant clos par rapport à la substitution de termes $S^0\,1$, $S^1\,1$, ... à des variables.

β) Par contre, bien que, par exemple, $\overline{1 + a} = \overline{Sa}$ soit une identité, ce qui est évident par récurrence sur a, la formule $1 + a = Sa$ n'est pas dérivable (dans $\mathscr{R}^+$) ; car toute formule dérivable est vraie dans la réalisation (ensembliste) suivante : les variables varient sur les ordinaux, les réalisations de 1, S, $+$ sont l'unité, le successeur, resp. l'addition usuelle des ordinaux. Or $1 + \omega \neq \omega + 1$.

On peut éliminer, d'une façon triviale, la notion abstraite d'ordinal, et ainsi donner une preuve combinatoire du fait que $1 + a = Sa$ n'est pas dérivable : les variables varient sur les couples ordonnés d'entiers $\langle p, q \rangle$, où $p \geqslant 0$, $q \geqslant 0$ et $p + q > 0$; on pose

$$\bar{1} = \langle 0, 1 \rangle, \qquad S(\langle n, m \rangle) = \langle n, m + 1 \rangle,$$

$$\langle n, m \rangle + \langle 0, q \rangle = \langle n, m + q \rangle$$

et

$$\langle n, m \rangle + \langle p + 1, q \rangle = \langle n + p + 1, q \rangle;$$

on a

$$\langle 0, 1 \rangle + \langle 1, 0 \rangle \neq \langle 1, 0 \rangle + \langle 0, 1 \rangle.$$

N. B. α) et β) établissent respectivement la validité (combinatoire) et et l'incomplétude du système $\mathscr{R}^+$ par rapport à la théorie combinatoire de l'addition. On voit donc l'ordre des choses : partant des règles mécaniques de l'addition (ici sous forme du système formel de (ii)) on s'aperçoit de leur caractère fonctionnel par le raisonnement de (iii) ; ensuite

on se donne un système formel contenant des variables (ici $\mathscr{R}^+$) et on se demande si oui ou non l'identité $\bar{t} = \bar{t'}$ équivaut à la dérivabilité de la formule $t = t'$ dans ce système. (Puisque le sens même de cette question repose sur une connaissance tout du moins partielle des notions de base combinatoires, un lecteur qui a suivi sans peine les preuves de α) et de β) peut espérer posséder cette connaissance).

On aura remarqué l'emploi d'une terminologie « psychologique » ce qui n'a rien d'étonnant puisque la théorie combinatoire est censée être idéaliste.

Enfin on notera que la constatation combinatoire, mais non mécanique :

La formule $1 + a = Sa$ *n'est pas dérivable dans* $\mathscr{R}^+$,

a le même caractère que l'identité $1 + a = Sa$ elle-même : à savoir, quel que soit la suite de formules du langage de $\mathscr{R}^+$ on constate mécaniquement si oui ou non elle est construite selon les règles de $\mathscr{R}^+$ (cf. : quel que soit l'entier n on calcule mécaniquement les valeurs de $1 + S^n 1$ et de $SS^n 1$) et aussi si oui ou non la dernière formule de la suite est identique à $1 + a = Sa$ (cf. : on constate si la valeur de $1 + S^n 1$ est $S^{n+1}1$). Le raisonnement de β) démontre que la réponse à l'une ou l'autre de ces questions sera négative.

Ce caractère *élémentaire* des *énoncés de non-dérivabilité formelle* sera essentiel pour tout ce qui suit.

a) *Langages et réalisations combinatoires.* On admettra les langages du calcul des prédicats avec égalité (App. I) modifiés comme suit : on supprime les quantificateurs (les variables de toutes les formules considérées sont donc libres) ; d'autre part la donnée du langage consiste en la donnée de fonctions combinatoires qui énumèrent, éventuellement avec des répétitions, les différentes sortes de symboles (on n'admet donc plus comme ensembles de symboles des ensembles disjoints quelconques). On se limitera souvent à des langages ne contenant qu'un nombre fini de constantes d'individus, de symboles fonctionnels et de symboles relationnels, et contenant une énumération particulière d'une suite (infinie) de variables.

N. B. Ces fonctions énumérantes, chacune donnée bien entendu par une description particulière, font partie de la donnée du langage : par conséquent on considérera comme différents deux langages dont les (descriptions des) fonctions énumérantes diffèrent, même si les ensembles énumérés sont identiques ; en particulier, on distinguera une énumération *finie* (dont la donnée est une suite finie, c'est-à-dire un objet combinatoire) d'une énumération *infinie* du même ensemble sans preuve combinatoire de leur équivalence. Ces distinctions viennent du fait que, contrairement aux cas d'objets considérés p. 189 dans (i), on ne peut toujours décider au moyen d'un raisonnement combina-

toire si oui ou non deux descriptions de fonctions sont équivalentes ni si deux fonctions énumèrent le même ensemble c'est-à-dire si les ensembles de leurs valeurs respectives sont identiques. Sur ce point la théorie combinatoire s'écarte de l'analyse ensembliste.

Soit $\mathscr{L}$ un langage (combinatoire). Une réalisation $\mathfrak{R}$ combinatoire de $\mathscr{L}$ est constituée par définition

(i) d'une énumération U (finie ou non finie) non vide d'objets combinatoires, appelée *univers* de $\mathfrak{R}$, ou *domaine* des variables,

(ii) d'un élément énuméré (c'est-à-dire parmi ceux énumérés) par U, pour chaque constante d'individu,

(iii) d'une fonction combinatoire à n variables (dont les arguments et les valeurs sont énumérés par U) pour chaque symbole fonctionnel à n variables,

(iv) d'une fonction caractéristique à n variables (ne prenant que deux valeurs distinctes, soient $\top$ et $\bot$) pour chaque symbole relationnel à n variables.

N. B. (iv) montre qu'on pourrait se confiner sans perte de généralité à des langages ne contenant que $=$ comme symbole relationnel. Si $\mathscr{L}$ contient une suite infinie de symboles fonctionnels, disons, à 2 variables, énumérée par la fonction φ définie sur U_0, on modifie la définition de réalisation comme suit : $\mathfrak{R}$ contient une fonction combinatoire Φ à 3 variables (la première variant sur U_0, les autres sur U), telle que, pour tout élément u_0 de U_0, la fonction $\Phi u_0 xy$ aux deux variables x et y est, par définition, la réalisation du symbole φu_0.

b) *Réalisation combinatoire d'une formule ; validité combinatoire.* Soit $\mathscr{L}$ un langage (combinatoire), $\mathfrak{R}$ une réalisation de $\mathscr{L}$ et A une formule de $\mathscr{L}$. On dira qu'une preuve combinatoire π réalise la formule A dans $\mathfrak{R}$ si, pour deux objets distincts, disons $\top$ et $\bot$, ou bien :

1° A est close, $\bar{A}$ est la valeur de A selon la valuation du calcul propositionnel [voir Chap.1] pourvu qu'on remplace $\bar{s} = \bar{t}$ par $\top$ si s et t désignent le même élément (énuméré par U) et par $\bot$ dans le cas contraire, et enfin π est un calcul mécanique constatant $\bar{A} = \top$; [on notera que la valuation du Chap. 1 est évidemment mécanique] ; ou bien,

2° les variables libres (et par conséquent toutes les variables) de A sont prises parmi $\{x_1, ..., x_n\}$ et π est une preuve combinatoire de *l'identité* $\overline{A_{\mathfrak{R}}}$:

Quels que soient les éléments $\bar{x}_1, ..., \bar{x}_n$ énumérés par U, le calcul de $\bar{A}$ selon le 1° aboutit à la valeur $\top$.

(En général, c'est-à-dire si U n'est pas une énumération finie, π n'est plus un calcul mécanique. On ne suppose évidemment pas que tout élément de U ait un nom dans $\mathscr{L}$, c'est-à-dire soit la réalisation d'un terme de $\mathscr{L}$.)

[Il est immédiat que, quel que soit $\mathfrak{R}$ on peut trouver une preuve (réalisation)

π de A si la formule $E \to A$ est valide au sens ensembliste, où E est la conjonction des axiomes d'égalité pour tous les termes figurant dans A. Inversement, si $E \to A$ n'est pas valide on peut trouver une réalisation $\mathfrak{R}$ du langage de A et des éléments $\bar{x}_1, ..., \bar{x}_n$ de l'univers de R tels que $\bar{A} = \perp$.]

Discussion. Des langages avec quantificateurs ne sont pas envisagés ici en raison de la difficulté suivante : les lois logiques usuelles ne sont pas valides pour les réalisations combinatoires, lorsque celles-ci sont étendues de façon naturelle aux formules quantifiées. Par exemple, pour une formule sans quantificateur $A(x_1, ..., x_n, x, y)$ il semble naturel de poser :

Le couple $(\pi, \bar{f})$ est une réalisation de $\wedge x \vee y\, A(x_1, ..., x_n, x, y)$ (formule où le symbole fonctionnel f à $n + 1$ variables n'apparaît pas) si $\bar{f}$ est une fonction combinatoire, et π réalise

$$A(x_1, ..., x_n, x, f(x_1, ..., x_n, x)) .$$

Le couple $(\pi, \bar{g})$ réalise $\vee x \wedge y \neg A(x_1, ..., x_n, x, y)$ (formule où le symbole fonctionnel g à n variables n'apparaît pas) si π réalise

$$\neg A(x_1, ..., x_n, g(x_1, ..., x_n), y) .$$

Le triplet $(\pi, \bar{f}, \bar{g})$ réalise $\wedge x \vee y\, A \vee \vee x \wedge y \neg A$ si π réalise

$$A(x_1, ..., x_n, x, f(x_1, ..., x_n, x)) \vee \neg A(x_1, ..., x_n, g(x_1, ..., x_n), y) ,$$

pour tout $n + 2$-uplet $\bar{x}_1, ..., \bar{x}_n, \bar{x}, \bar{y}$ du domaine considéré.

Il n'y a aucune raison de penser que $\wedge x \vee y\, A \vee \vee x \wedge y \neg A$ est nécessairement réalisée en ce sens (bien qu'elle soit valable au sens ensembliste).

En fait, il n'est même pas plausible qu'il existe deux fonctions $\bar{f}$ et $\bar{g}$ définies *mécaniquement*, telles que :

ou bien $$A(x_1, ..., x_n, x, f(x_1, ..., x_n))$$
ou bien $$\neg A(x_1, ..., x_n, g(x_1, ..., x_n)\, y)$$

sont vrais
au sens ensembliste (cf. la section *c*).

c) *Traductions ensemblistes d'identités combinatoires* ; *démonstrations non combinatoires de ces traductions.* Evidemment, on suppose connues *à la fois* les notions ensemblistes et les notions combinatoires dans cette section. Les fondements combinatoires n'en dépendent pas, mais les notions qu'elle présente serviront à rendre *intelligibles* les démarches purement combinatoires du paragraphe suivant.

A tout langage combinatoire $\mathscr{L}$ et toute réalisation combinatoire $\mathfrak{R}$ de $\mathscr{L}$, on va associer de façon naturelle un langage $\mathscr{L}^*$ et une réalisation $\mathfrak{R}^*$ de $\mathscr{L}^*$, au sens de la Partie A, pp. 159 et 160.

Les objets combinatoires de $\mathscr{L}$ et $\mathfrak{R}$ (symboles, alphabet et mots de $\mathfrak{R}$) sont considérés comme des ensembles ; en particulier un mot est l'ensemble : suite ordonnée de ses lettres ; $\mathscr{L}$ et $\mathfrak{R}$ étant constitués par des suites d'énumérations et de fonctions combinatoires des objets précédents, on associe à chaque énumération l'ensemble des objets énumérés, et à chaque fonction combinatoire, son graphe (faisant abstraction des définitions particulières par lesquelles ces ensembles nous sont donnés) ; on définit ainsi :

$\mathscr{L}^*$, suite des ensembles des divers types de symboles, et

$\mathfrak{R}^*$, dont l'univers est l'ensemble des mots appartenant au domaine de $\mathfrak{R}$, la réalisation d'un symbole de fonction f (resp. de relation R) étant l'ensemble associé à $\overline{f}_{\mathfrak{R}}$ (resp. $\overline{R}_{\mathfrak{R}}$).

Les propriétés de la correspondance $(\mathscr{L}, \mathfrak{R}) \Rightarrow (\mathscr{L}^*, \mathfrak{R}^*)$ montrent le rôle essentiel des définitions particulières de fonctions et d'énumérations pour les notions de langage et de réalisation combinatoires :

1° il existe des langages et des réalisations ensemblistes qui ne peuvent pas être associés de la manière décrite à un langage et une réalisation combinatoires,

2° il existe des réalisations combinatoires qui sont équivalentes du point de vue ensembliste (c'est-à-dire auxquelles est associée la même réalisation ensembliste) mais pas du point de vue combinatoire (c'est-à-dire que l'équivalence ci-dessus ne peut être définie et démontrée combinatoirement) ; autrement dit, la correspondance ci-dessus n'a pas de réciproque uniquement définie (le lecteur devrait comparer ceci avec la nécessité d'un choix canonique de définitions d'objets de la s. c. t., dans la Partie A, Lemme 3),

1° est une conséquence évidente de ce résultat de la théorie des fonctions récursives : il existe des ensembles non énumérables par des fonctions mécaniquement définissables et à plus forte raison par des fonctions combinatoires.

2° résulte d'une analyse plus délicate des preuves combinatoires, qui montre l'existence de deux fonctions combinatoires ayant même graphe, mais telles qu'on ne puisse montrer combinatoirement cette propriété.

A étant une formule de $\mathscr{L}$, dont les variables sont parmi $x_1, ..., x_n$, une *traduction* de l'identité combinatoire $\overline{A}_{\mathfrak{R}}$ (c'est-à-dire : « A est satisfaite par $\mathfrak{R}$ ») est simplement une formule de $\mathscr{L}_E$ exprimant :

$$\text{« } \wedge x_1, ..., \wedge x_n \ A \text{ est satisfaite par } \mathfrak{R}^* \text{ ».}$$

Il est clair que si $\wedge x_1 ... \wedge x_n A$ n'est pas satisfaite par $\mathfrak{R}^*$, il n'y a pas de réalisation combinatoire de A dans $\mathfrak{R}$.

On peut formuler ainsi les grandes lignes des démonstrations non combinatoires (de traductions) d'identités combinatoires :

D'abord (cas élémentaire), on peut considérer les interprétations, *dans la réalisation* $\mathfrak{R}^*$, de formules quantifiées de $\mathscr{L}^*$ (auxquelles on n'a pas assigné

de sens combinatoire) et en leur appliquant des principes qui sont valables pour l'interprétation ensembliste de $\mathscr{L}^*$, obtenir $\Lambda x_1 \ldots \Lambda x_n\ A$. Ce genre de démonstration nous est familier en arithmétique ou en théorie des suites d'entiers, où on l'appelle couramment « démonstration » non constructive, cf. p. 181-182.

En second lieu, on peut plonger $\mathfrak{R}^*$ dans une réalisation qui n'est associée à aucune réalisation combinatoire, et se servir des propriétés de cette réalisation étendue. Ceci nous est familier en théorie analytique des nombres, où la structure des nombres naturels (sous-ensemble de C_ω dans la Partie A) est plongée dans le plan complexe ($\subset C_{\omega+1}$) ou dans l'espace des fonctions du plan complexe ($\subset C_{\omega+2}$). Dans un exemple très simple de ce procédé, en p. 192, on se sert de la structure des ordinaux pour démontrer un résultat de non-dérivabilité sur le système formel $\mathscr{R}^+$, résultat qui est une identité de la sorte ici considérée.

Dans ce dernier cas, pour ainsi dire la simple lecture de la démonstration montre comment éviter l'usage de la structure essentiellement non combinatoire des ordinaux : à la place des ordinaux, l'on considère ω^2, et sur ω^2 un ordre pour lequel on montre les propriétés utilisées des ordinaux. De même, un examen des démonstrations existantes de théorie analytique des nombres montre qu'au prix de détails supplémentaires, on peut éviter complètement l'introduction de réalisations non combinatoires $\langle C_{\omega+1}, \in_{\omega+1} \rangle$ ou $\langle C_{\omega+2}, \in_{\omega+2} \rangle$, en se confinant au plan rationnel complexe et en utilisant des approximations des fonctions étudiées.

Par contre il n'y a pas évidence du tout que l'usage suivant de réalisations abstraites soit évitable : considérez les règles de déduction à partir de $\mathscr{A}^*$, $\overline{D}$ (cf. p. 176, (i) et (iii)) et l'identité : « $A \wedge \neg A$ n'est pas formellement dérivable par les règles $\overline{Dem}$ » (pour une formule donnée A). $\mathscr{A}^*$ étant satisfait par $\langle C_{\omega+\omega}, \in_{\omega+\omega} \rangle$, toutes les conclusions de $\overline{D}$ le sont aussi, parce que les règles préservent la validité dans les réalisations ensemblistes ; $A \wedge \neg A$ étant fausse dans $\langle C_{\omega+\omega}, \in_{\omega+\omega} \rangle$ n'est donc pas dérivable.

Discussion : Quoique simple, cet argument n'est pas vide parce qu'il dépend de la vérification que $\mathscr{A}^*$ est satisfait par $\langle C_{\omega+\omega}, \in_{\omega+\omega} \rangle$: si l'axiome 3* est remplacé par l'axiome de compréhension non restreint (qui est évidemment faux dans $\langle C_{\omega+\omega}, \in_{\omega+\omega} \rangle$), l'identité correspondante est fausse (cf. Partie A, p. 166).

Le fait que plonger une structure $\mathfrak{S}$ dans une structure plus riche conduit souvent à des démonstrations plus simples au sujet de $\mathfrak{S}$ est bien connu dans les mathématiques modernes. Ici on se sert de $\langle C_{\omega+\omega}, \in_{\omega+\omega} \rangle$ pour dériver un résultat sur $\langle C_\omega, \in_\omega \rangle$ grâce au développement de l'arithmétique dans $\langle C_\omega, \in_\omega \rangle$ (cf. Partie A). Justement parce que cette démonstration est si simple, n'utilisant des règles formelles que leur propriété de préserver la vérité, il n'est pas du tout plausible qu'elle puisse être *facilement* transformée en

démonstration combinatoire, contrairement à la démonstration citée précédemment.

Avec les explications informelles fournies par cette section, la brève exposition ci-dessous des problèmes posés par les fondements combinatoires doit être tout à fait compréhensible.

1. Comment analyse-t-on les mathématiques intuitives au moyen des notions de bases combinatoires ?

Comme une bonne part des mathématiques intuitives s'occupe d'objets abstraits tels que $\langle C_\alpha, \in_\alpha \rangle$, $\alpha \geqslant \omega$, qui ne sont pas du tout combinatoires, l'analyse ne peut porter sur les objets eux-mêmes ; on peut alors de façon cohérente la faire porter sur les raisonnements *concernant* ces objets. Cette possibilité est formulée de façon précise dans le *programme de Hilbert.*

a) *Représentation* (description) *des raisonnements mathématiques au moyen de systèmes formels.* — Au début de l'introduction était précisé qu'on ne sait pas codifier au moyen de règles mécaniques, le passage du raisonnement intuitif à sa formulation dans un langage formel. En effet on cherche une représentation fidèle du sens, non de la forme extérieure (des mots) du raisonnement intuitif. Et, supposé ce passage accompli (faisant partie des données), il reste encore à définir combinatoirement les relations de base du raisonnement intuitif (par exemple la relation de conséquence), ou plutôt les relations correspondantes pour la représentation du raisonnement, et il reste à démontrer combinatoirement leurs propriétés.

Dans *b*) et *d*) sera formulé exactement ce qu'il faut établir, sous forme de *conditions combinatoires d'adéquation.* Pour l'essentiel *b*) correspond à $E^{\mathscr{A}s}$ et *d*) à $U^{\mathscr{A}s}$ (cf. Partie A, p. 160). Comme il fallait s'y attendre, les Théorèmes 4 et 5 (ou plutôt des généralisations adéquates) sont décisifs pour les résultats qui sont résumés § 4, a), b).

Discussion. — Pour bien suivre la discussion § 4, le lecteur devrait comparer le rôle, (i), du résultat : $\overline{D} = \overline{V}$ (ou plus généralement du Théorème 5) pour les fondements combinatoires, et celui, (ii), de résultats correspondants pour les fondements ensemblistes.

(i) Si l'on *accepte* les notions ensemblistes à la base de la définition de la relation de conséquence, le Théorème 5 fournit une *démonstration mathématique* que celle-ci coïncide avec une certaine relation définie combinatoirement, ceci pour les formules du premier ordre. Mais si l'on se confine au cadre combinatoire on ne dispose que du fait empirique : il se trouve que chaque formule du premier ordre de $\mathscr{L}_E$ reconnue pour valide logiquement est engendrée au moyen de certaines règles formelles (celles du Lemme 3, cf. p. 176, (i) et (iii)). [De même, à l'aide de la théorie des fonctions récursives, et *en acceptant* les

notions ensemblistes, on montre que la relation de conséquence du second ordre n'est pas définissable par des règles mécaniques. Dans le cadre combinatoire on ne peut même pas formuler ce fait, à fortiori le démontrer. On peut seulement dire que l'on ne *connaît* pas une telle définition ; et pour tout cas particulier de ce fait général exhiber un contre-exemple.]

(ii) Un résultat correspondant pour les fondements ensemblistes, disons de la théorie intuitive de l'arithmétique **N**, serait une *démonstration* que **N** satisfait les axiomes de Peano $\mathscr{A}_{\mathbf{N}}$. A l'intérieur du cadre ensembliste, $\mathscr{A}_{\mathbf{N}}$ est simplement une donnée ; on ne peut exprimer le raisonnement qui montre que **N** satisfait $\mathscr{A}_{\mathbf{N}}$, et doit se contenter d'admettre une terminologie informelle adaptée.

b) *Réduction de principes intuitifs à des principes combinatoires* (le problème de la non-contradiction d'Hilbert). — Une *exigence minimale* pour cette réduction peut être formulée avec la notion de traduction décrite dans § 0 c) :

Soient $\mathscr{L}$ un langage et $\mathfrak{R}$ une réalisation combinatoire (réalisant $\mathscr{L}$). Pour chaque formule A de $\mathscr{L}$, soit A_T la traduction *canonique* de $\overline{A_{\mathfrak{R}}}$. On veut savoir, au moins pour les formules closes A :

(i) si A est réalisé dans $\mathfrak{R}$, y a-t-il une dérivation formelle de A_T à partir de $\mathscr{A}^*$ (ou même d'un sous-ensemble de $\mathscr{A}^*$) ?

(ii) s'il y a une dérivation formelle de A_T, est-ce que A est réalisé (au sens combinatoire) dans $\mathfrak{R}$?

Ces questions étant ainsi formulées, la recherche d'une solution purement combinatoire a au moins un sens. Précisément : supposons (p. ex. si $\mathfrak{R} = \mathfrak{R}_C$ et $\mathscr{L} = \mathscr{L}_C$, voir pp. 204-205) l'existence d'une formule Dem $(s, \ulcorner A_T \urcorner)$ qui définit dans $\mathfrak{R}$ la relation combinatoire : « la suite s de formules de $\mathscr{L}_E$ est une dérivation formelle de A_T à partir de $\mathscr{A}^*$ » ; une réponse à la question (i) est une fonction combinatoire f dont l'argument est une formule de $\mathscr{L}$ et l'image une suite de formules de $\mathscr{L}_E$, avec une démonstration combinatoire de l'identité :

$$\overline{A_{\mathfrak{R}} \rightarrow \mathrm{Dem}(fA, \ulcorner A_T \urcorner)} \, .$$

Cette réponse revient à établir effectivement que les mathématiques combinatoires peuvent être développées dans la théorie des ensembles ; ce qui était déjà utilisé dans le Lemme 4, de la Partie A.

La question (ii) prend simplement la forme (s variant sur les suites finies de formules de $\mathscr{L}_E$, et pour toute formule close A de $\mathscr{L}$) :

Y a-t-il une preuve combinatoire de

$$\overline{\mathrm{Dem}(s, \ulcorner A_T \urcorner) \rightarrow A_{\mathfrak{R}}} \ ?$$

Notez que le caractère combinatoire de la relation $\overline{\text{Dem}}$ est essentiel pour une formulation combinatoire des deux questions.

Une solution positive de (ii) constitue une vraie *élimination des hypothèses ensemblistes*, car une démonstration combinatoire de

$$\overline{\text{Dem}\,(s, \ulcorner A_T \urcorner) \to A_{\mathfrak{R}}}$$

n'utilise pas le sens (c'est-à-dire la réalisation) des formules de $\overset{*}{s}$ — pour la bonne raison que celui-ci n'est pas du tout combinatoire —, mais seulement leurs propriétés (formelles) syntaxiques.

Par contre la justification *intuitive* de l'affirmation

$$\overline{\text{Dem}\,(s, \ulcorner A_T \urcorner) \to A_{\mathfrak{R}}}$$

est tout juste celle de la démonstration de consistance à la fin du § 0, c) : on considère le sens des formules de s, conclu comme au § 0, c) qu'elles sont vraies, donc aussi A_T, et donc $\overline{A_{\mathfrak{R}}}$, du moins si A est close. Evidemment, cet argument disparaît si l'on n'accepte pas les vérités ensemblistes exprimées par $\mathscr{A}^*$.

> *Discussion.* Les lignes précédentes montrent qu'il ne peut être question de réduction combinatoire si une solution positive n'est pas donnée à (ii) : sinon même les conclusions purement combinatoires tirées d'hypothèses ensemblistes ne seraient pas combinatoirement justifiées. Mais cette solution est aussi tout ce qu'on peut exiger au stade présent de l'analyse, parce que les formules A_T sont les seules auxquelles un sens combinatoire est attaché (une extension est *possible* si l'on étend la notion de réalisation combinatoire d'une façon moins naïve que p. 195). Le Théorème 4 de la Partie A rend implausible même au premier abord une solution positive de (ii) (cf. § 3 pour des détails). *Mais la question* (ii) *a un sens pour, au lieu de* $\mathscr{A}^*$, *tout système formel qui représente les raisonnements sur une structure abstraite*, pourvu qu'une notion sensée de traduction des formules combinatoires soit définie.
>
> Il n'y a donc pas de réfutation *générale* du programme de Hilbert pourvu qu'il existe un système formel à priori non combinatoire (plus généralement non constructif) pour lequel (ii) a une solution positive. Un tel système est donné dans la section *c*). (Ceci répond à la doctrine positiviste mentionnée en fin d'Introduction ; nous y reviendrons au § 4 c).)

Remarque sur le problème de la non-contradiction de Hilbert. — La non-contradiction affirme que, pour tout B de $\mathscr{L}_E$, et lorsque les variables x, y ont pour domaine les suites de formules de $\mathscr{L}_E$,

$$(+)\ \text{Dem}\,(x, \ulcorner B \urcorner) \to \neg\, \text{Dem}\,(y, \ulcorner \neg\, B \urcorner)\ ;$$

ou, si $\perp$ dénote la traduction d'une formule combinatoire fausse telle que $0 = 1$:

$$(++) \quad \neg \, \mathrm{Dem}\,(x, \ulcorner \perp \urcorner)\,;$$

avec

$$(0 = 1)_T = \vee y_1 \vee y_2 [\wedge u \neg (u \in y_1) \wedge \wedge u (u \in y_2 \leftrightarrow u = y_1) \wedge y_1 = y_2]$$

$(+)$ et $(++)$ sont équivalents puisque toute formule est formellement dérivable à partir d'une formule fausse. Et, si (i) est satisfait, (ii) *est équivalent* (*combinatoirement*) *à* $(+)$.

D'abord $(++)$ est le cas particulier de (ii) où A est $0 = 1$.
Réciproquement, d'après (i) :

$$\overline{\neg A_{\mathfrak{R}} \rightarrow \mathrm{Dem}\,[f(\neg A), \ulcorner(\neg A)_T\urcorner]}\ ;$$

donc

$$\overline{\neg \, \mathrm{Dem}\,[f(\neg A), \ulcorner(\neg A)_T\urcorner] \rightarrow \neg \neg A_{\mathfrak{R}}}$$

et

$$\overline{\neg \, \mathrm{Dem}\,[f(\neg A), \ulcorner(\neg A)_T\urcorner] \rightarrow A_{\mathfrak{R}}}\ .$$

En combinant ceci avec le cas particulier de $(+)$, où B est A_T, y est $f(\neg A)$. on obtient :

$$\overline{\mathrm{Dem}\,[x, \ulcorner A_T \urcorner] \rightarrow A_{\mathfrak{R}}}\ .$$

L'avantage de $(++)$ sur (ii) réside principalement dans le remplacement d'une variable (sur les formules de $\mathscr{L}$) de (ii) par la constante $\perp$. Mais la signification de ces deux conditions équivalentes est mieux en évidence sous forme de la condition d'adéquation (ii) (cf. discussion de cette section, ci-dessus).

c) *Résultats positifs sur le problème de Hilbert* (ces résultats étant formulés et prouvés en théorie des démonstrations, nous ne pouvons que les indiquer ici).

Soit un langage $\mathscr{L}$ au sens du § 0 b), A une formule de $\mathscr{L}$, de variables parmi $x_1, ..., x_n$, et π une réalisation de A (c'est-à-dire une réalisation de $\mathscr{L}$, et une preuve combinatoire de A pour cette réalisation).

Résultat faible (« faible » pour les fondements combinatoires parce que sa formulation utilise à la fois les notions combinatoires *et* ensemblistes). Si les variables de la formule B de $\mathscr{L}$, sont parmi $y_1, ..., y_n$, *et si* (la formule de $\mathscr{L}^*$) $\wedge y_1 ... \wedge y_n$ *B est conséquence ensembliste de* $\wedge x_1 ... \wedge x_n$ *A*, *alors il existe une preuve combinatoire de B pour la réalisation donnée de* $\mathscr{L}$.

La clef de la démonstration est la propriété *combinatoire* de la formalisation *particulière* de la relation de conséquence indiquée dans la Partie A, Lemme 3 (voir également (i), page 198) : si (pour des formules purement universelles) $\bigwedge y_1 \ldots \bigwedge y_m B$ est déduite *par ces règles* de $\bigwedge x_1 \ldots \bigwedge x_n A$, alors il existe une déduction purement propositionnelle de B à partir d'une conjonction $A_1 \wedge \cdots \wedge A_k$ de formules A_i venant de la substitution de certains termes aux variables de A. D'après p. 194, une telle déduction *définit* une preuve cômbinatoire de $A_1 \wedge \cdots \wedge A_k \rightarrow B$ qui, jointe à la réalisation de A, est aussi une réalisation de B.

La propriété particulière de ces règles n'est pas satisfaite par les formalisations courantes comme celle de Bourbaki. Par exemple, si *modus ponens* (de X et $X \rightarrow Y$ déduire Y) fait partie des règles, une dérivation de B à partir de $\bigwedge x_1 \ldots \bigwedge x_n A$ peut contenir des formules avec alternances de quantificateurs ; or, nous avons vu en § 0, *b*) que si la notion de réalisation combinatoire est étendue de façon « naturelle », les règles formelles (comme $A \vee \neg A$) ne sont pas combinatoirement valides.

Version combinatoire. Dans ce cas, la notion de conséquence ensembliste doit être remplacée par la relation combinatoire suivante, notée $\overline{\mathrm{Dem}_F (s, X)}$: on énumère toutes les règles de déduction formelles qui paraissent évidemment valides, comme *modus ponens* (cf. section *a*) du présent paragraphe) ; $\overline{\mathrm{Dem}_F (s, X)}$ est la relation : la suite s de formules de $\mathscr{L}^*$ est une dérivation formelle de la formule X de $\mathscr{L}^*$, au moyen des règles formelles énumérées. Soit $\mathrm{Dem}_S (s, X)$ la relation correspondant à $\mathrm{Dem}_F (s, X)$, pour les règles de déduction *spéciales* de la première version. Celle-ci utilisait l'équivalence entre $\overline{\mathrm{Dem}_S}$ et la relation de conséquence ensembliste. Pour la version combinatoire, il faut utiliser à la place l'équivalence entre $\overline{\mathrm{Dem}_S}$ et $\overline{\mathrm{Dem}_F}$ (équivalence *combinatoire*), laquelle est vérifiée dans la théorie des démonstrations : il existe une fonction combinatoire f telle que $\overline{\mathrm{Dem}_F (s, X) \rightarrow \mathrm{Dem}_S (fs, X)}$ est combinatoirement démontrable (l'implication réciproque est évidente puisque les règles de déduction spéciales font partie de celles de Dem_F).

Notez que la première version, jointe à la complétude de $\overline{\mathrm{Dem}_S}$, permet seulement de démontrer ceci : il y a une règle mécanique définissant une fonction f pour laquelle la *traduction* de $\overline{\mathrm{Dem}_F (s, X) \rightarrow \mathrm{Dem}_S (fs, X)}$ est *vraie*. A savoir : étant donnés s et X, décider si $\mathrm{Dem}_F (s, X)$ est vrai ; sinon l'implication est satisfaite ; si $\overline{\mathrm{Dem}_F (s, X)}$ est vraie, X est valide ; énumérer les dérivations formelles de S jusqu'à obtention d'une dérivation de X (il y en a nécessairement une parce que tous les théorèmes de F sont valides et tous les théorèmes valides sont formellement dérivables dans S).

Mais cet argument laisse de côté la question de savoir s'il y a une

fonction *combinatoire* f et, si pour cet f, l'affirmation peut être combinatoirement démontrée. Non seulement il y a une différence conceptuelle entre les deux résultats, mais encore les méthodes mathématiques qu'ils utilisent sont tout à fait différentes.

Discussion. Les résultats ci-dessus permettent d'éliminer les démonstrations non constructives élémentaires au sens du §0c), p. 196. Ce qui couvre certainement une partie non triviale des mathématiques courantes (qui se présente sous une forme non combinatoire). Dans le cas de l'Arithmétique, ceci s'applique aux résultats démontrables dans le système suivant : on part des axiomes courants (Chap. 3, Ex. 2 d)) ; on peut rajouter des symboles de fonctions, et comme axiomes des équations pour lesquelles existe une réalisation combinatoire (par exemple $f(0, y) = 1$ et $f(x + 1, y) = y.f(x, y)$ pour l'exponentielle y^x).

Mais, (i) *il faut restreindre le schéma d'induction à des formules purement universelles A* (de $\mathscr{L}^*$) puisque, (ii) pour d'autres A nous n'avons pas d'extension qui nous convienne de la notion de réalisation combinatoire. En ce qui concerne (i), si Ax est, disons $\bigwedge y B(x, y)$,

$$A0 \wedge \bigwedge z[Az \to A(z + 1)] \to \bigwedge x Ax$$

est une conséquence formelle de

$$\bigwedge x \bigwedge y \{ [B(0, y) \wedge \bigwedge z[B(z, y) \to B(z + 1, y)]] \to B(x, y) \}$$

et ceci est conséquence de

$$\bigwedge x \bigwedge y \{ [B(0, y) \wedge (\bigwedge z < x) [B(z, y) \to B(z + 1, y)]] \to B(x, y) \} .$$

Pour cette formule il y a une réalisation combinatoire, car si $B(x, y)$ est une relation combinatoire, il en est de même de $(\bigwedge z < x) [B(z, y) \to B(z + 1, y)]$, les variables ayant pour valeurs des entiers naturels.

En ce qui concerne (ii), le lecteur notera que de garder le schéma d'induction pour d'autres formules A quelles qu'elles soient est tout à fait inacceptable tant que l'on n'a pas défini de réalisation combinatoire des formules qui figurent dans ces cas du schéma d'induction. Et que, par contre, du point de vue des fondements ensemblistes, la restriction (ii) est tout à fait artificielle (cf. note 4 de la Partie A).

d) *Réduction de principes intuitifs à des principes combinatoires* (suite). Une structure intuitive S et son langage, $\mathscr{L}_S$, étant donnée, une sorte d'exigence *maximale* pôur des fondements combinatoires de S est de trouver un système formel qui est combinatoirement défini, valide et *saturé* pour S vis-à-vis de $\mathscr{L}_S$. Car les fondements combinatoires concernent les raisonnements *sur* S et un tel système formel déciderait toutes les questions (formulées dans $\mathscr{L}_S$) sur S.

Le Chapitre 4 en contient plusieurs exemples [surtout du premier ordre] malgré le fait (cf. Ex. 1, Chap. 3) qu'aucun d'entre eux n'est catégorique

(cf. Partie A, p. 161 (ii)). Noter que le résultat de non-catégoricité pour l'arithmétique de l'Exercice 2, Chapitre 3 n'a pas d'intérêt pour les fondements combinatoires, alors que le Théorème 4 de la Partie A montre que même le système formel $\mathscr{A}^*$ ne satisfait pas l'exigence maximale vis-à-vis des assertions arithmétiques, en particulier des traductions (au sens du § 0 c) d'assertions combinatoires.

La théorie des fonctions récursives permet de formuler et de prouver une généralisation très concluante du Théorème 4 : *il n'y a pas d'extension consistante de $\mathscr{A}^*$ dont l'ensemble d'axiomes soit définissable au moyen d'une règle mécanique, qui soit saturée vis-à-vis des assertions arithmétiques.*

2. Comment trouve-t-on des lois (axiomes) ou les notions de base combinatoires ?

On utilisera ci-dessous quelques notations de A, § 2*a*.

a) Le lecteur peut s'orienter sommairement au sujet de ce problème en faisant correspondre le mélange des notions différentes d'ensemble au mélange des espèces de preuves dites constructives : en particulier, la structure (i) des ensembles héréditairement finis aux calculs mécaniques ; l'échelle des types (ii) aux preuves combinatoires ; les propriétés abstraites (iii) aux preuves dites intuitionnistes. On n'insiste pas ici sur les détails de cette comparaison parce que les connaissances du lecteur des notions correspondantes ne sont guère symétriques : il connaît mieux la notion (ii) que les notions combinatoires, et, en revanche, la littérature intuitionniste est beaucoup plus riche que celle sur la logique des propriétés abstraites ; voir § 3 fin.

b) Le *langage de base* $\mathscr{L}_C$ et sa *réalisation* $\mathfrak{R}_C$ (« C » pour : « combinatoire » ou encore, « concaténation », c'est-à-dire : mise bout à bout). $\mathscr{L}_C$ est constitué par un seul symbole relationnel ($=$), deux constantes d'individu 0 et 1 (ou $\top$ et $\bot$), deux symboles fonctionnels s_0 et s_1 à une seule variable, et une suite de symboles fonctionnels $f_1, f_2, ...,$ à deux variables.

L'univers de $\mathfrak{R}_C$ consiste en suites finies de deux objets concrets ; les réalisations $\bar{0}$ et $\bar{1}$ sont les deux suites constituées d'un seul élément ; $\bar{s}_0$ et $\bar{s}_1$ sont les fonctions combinatoires qui attachent $\bar{0}$ resp. $\bar{1}$ à la fin d'un élément de l'univers ; $\bar{f}_i$ $(i = 1, 2, ...)$ sera définie à partir des règles de *c*) ci-dessous.

N. B. Suffisance de $\mathscr{L}_C$ et $\mathfrak{R}_C$ au point de vue de la *définissabilité* (correspondant dans l'analyse ensembliste à $X^{\mathscr{A}s}$, cf. A, § 1, p. 160). On trouvera un exposé systématique dans la monographie de Smullyan, *Theory of Formal Systems*, Princeton (1961) qui définit, entre autres, les fonctions à un nombre fini de variables et les mots d'un alphabet à un nombre fini de lettres. (Le lecteur vérifiera lui-même le caractère combinatoire de ces définitions parce que l'auteur ne fait pas attention explicitement à cette question.) En particulier le langage $\mathscr{L}_C$

peut lui-même être défini dans $\mathfrak{R}_C$ au moyen de formules de $\mathscr{L}_C$ (cf. Théorème 4, Partie A) de façon qu'une suite de symboles de $\mathscr{L}_C$ soit la concaténée des éléments (suites) de l'univers $\mathfrak{R}_C$ qui leur sont associés.

Exemple. Si on prend (la suite) $\langle \bar{0}\,\bar{1} \rangle$ pour la constante 0, $\langle \bar{0}\,\bar{1}\,\bar{1} \rangle$ pour 1, et $\langle \bar{0}\,\bar{1}\,\bar{1}\,\bar{1} \rangle$ pour $=$, alors la formule $0 = 1$ est la suite $\langle \bar{0}\,\bar{1}\,\bar{0}\,\bar{1}\,\bar{1}\,\bar{1}\,\bar{0}\,\bar{1}\,\bar{1} \rangle$ qui est définie par le terme

$$s_1\, s_1\, s_0\, s_1\, s_1\, s_1\, s_0\, s_1\, 0\,.$$

On voit que ces définitions des symboles 0, 1, et $=$ permettent de retrouver la suite de symboles à partir de l'objet que ce code lui associe, ce qui serait impossible si, par exemple, on associait $\langle \bar{0} \rangle$ à 0 et $\langle \bar{1} \rangle$ à 1 ; car quel que soit l'objet a associé au symbole relationnel $=$, étant une suite des objets $\bar{0}$ et $\bar{1}$, a serait aussi associé à une suite de constantes d'individu.

c) *Un système formel $\mathscr{S}_C$, formulé dans $\mathscr{L}_C$ et valide dans $\mathfrak{R}_C$.* On admet toutes les règles qui sont valides pour toutes les réalisations combinatoires, voir § 0*b*). De plus on a :

(i) les axiomes des successeurs :

$$s_0\, x = s_0\, y \to x = y\,, \quad s_1\, x = s_1\, y \to x = y\,, \quad \neg\, s_0\, x = x\,, \quad \neg\, s_1\, x = x\,,$$

$$\neg\, s_0\, x = s_1\, y\,, \quad \neg\, s_0\, x = 0\,, \quad \neg\, s_0\, x = 1\,, \quad \neg\, s_1\, x = 0\,, \quad \neg\, s_1\, x = 1\,;$$

(ii) le schéma de démonstration par récurrence : pour toute formule Ax de $\mathscr{L}_C$, on déduit Ax de

$$A\,0 \wedge A\,1 \wedge (Ax \to As_0x) \wedge (Ax \to As_1x)\,;$$

Ecrivant $C^n = \{\, 0, 1, s_0, s_1, f_r : r < n \,\}$ $(n = 1, 2, \ldots)$ on se donne une énumération $(u_0^n, u_1^n, v_0^n, v_1^n)$ de tous les quadruplets (u_0, u_1, v_0, v_1), où les termes u_0, u_1 sont construits sur $\{\, y \,\} \cup \bigcup_n C^n$ et v_0 et v_1 sur $\{\, x, y, z \,\} \cup \bigcup_n C^n$, énumération telle que u_0^n et u_1^n sont construits sur $\{\, y \,\} \cup C^n$ et v_0^n et v_1^n sur

$$\{\, x, y, z \,\} \cup C^n\,.$$

On écrit $v[z]$ pour v. Alors on admet les axiomes :

(iii) $\quad f_n(0, y) = u_0^n\,, \quad f_n(1, y) = u_1^n\,, \quad f_n(s_0\, x, y) = v_0^n[f_n(x, y)]$

et

$$f_n(s_1\, x, y) = v_1^n[f_n(x, y)]\,.$$

La validité de (i) (pour $\mathfrak{R}_C$) est évidente ; (ii) se vérifie par récurrence (d'où le nom de ce schéma). Il reste à considérer (iii) ; on va voir que la réalisation constituée par l'univers de $\mathfrak{R}_C$, $\bar{0}$, $\bar{1}$, $\bar{s}_0$, $\bar{s}_1$ peut être complétée d'une seule façon en une réalisation qui satisfait (iii) : les règles mécaniques qui font partie des fonctions $\bar{f}_n$ réalisant f_n, ne sont autres que celles définies, au sens du § 0*a*) (ii), par les axiomes (iii) eux-mêmes ; le caractère fonctionnel de ces règles (sur l'univers de $\mathfrak{R}_C$) se démontre par récurrence : voir § 0*a*) (iii).

N. B. Cette preuve de la validité de $\mathscr{S}_C$ illustre la relation entre les preuves combinatoires en tant que pensées et les dérivations formelles : il faut avoir saisi la méthode de preuve par récurrence pour se convaincre de la validité des règles formelles qui sont censées décrire ces preuves.

En ce qui concerne la suffisance de $\mathscr{S}_C$ pour formuler les *démonstrations* de la pratique mathématique combinatoire on trouvera les détails dans les textes sur la théorie de démonstration : par exemple la solution partielle du problème de Hilbert mentionnée § 1*c*) ne réclame que les principes formulés dans $\mathscr{S}_C$. Le rôle de ce système pour les mathématiques combinatoires peut donc être comparé à celui des axiomes de Zermelo (A, § 2), pour la pratique ensembliste.

d) *Est-ce que $\mathscr{S}_C$ axiomatise la théorie combinatoire de $\mathfrak{R}_C$?* $\mathscr{S}_C$ est évidemment insuffisante pour définir toutes les fonctions combinatoires sur l'univers de $\mathfrak{R}_C$: en fait, la preuve combinatoire de la validité de $\mathscr{S}_C$, donnée ci-dessus, permet d'énumérer les fonctions $\bar{f}_n$, bien entendu par une fonction combinatoire, d'où, en appliquant la méthode diagonale de Cantor, une fonction combinatoire différente de chacune des fonctions définies dans $\mathscr{S}_C$.

On obtient sans peine une formule du langage $\mathscr{L}_C$ lui-même qui est valide, mais qui n'est pas démontrable en $\mathscr{S}_C$: la méthode de Gödel (Théorème 4 de la Partie A), dégagée de son application particulière à une théorie des ensembles, montre que

$$\neg \text{Dem}(x, s^*)$$

n'est pas *démontrable* en $\mathscr{S}_C$ où, pour une définition de $\mathscr{L}_C$ donnée (voir (*b*) ci-dessus), Dem (x, y) est la relation (combinatoire) : $\bar{x}$ est une suite de formules construites selon les règles de $\mathscr{S}_C$ et $\bar{y}$ est la dernière formule de $\bar{x}$; et s^* est la définition canonique de la formule $0 = 1$, c'est-à-dire de l'élément de l'univers qui est la formule notée $0 = 1$ d'après la définition du langage $\mathscr{L}_C$ choisie.

D'autre part, la preuve de la validité de $\mathscr{S}_C$ montre que $\neg$ Dem (x, s^*) est valide dans $\mathfrak{R}_C$.

La preuve de la validité de $\mathscr{S}_C$ établit aussi la validité du schéma suivant dont la formule $\neg$ Dem (x, s^*) est un cas particulier (avec $0 = 1$ au lieu de A) :

Pour toute formule A de $\mathscr{L}_C$ soit s_A sa description canonique (partant de la définition de $\mathscr{L}_C$ considérée) ; alors

$$\text{Dem}\,(x, s_A) \to A$$

est valide. Ce schéma, formulé en $\mathscr{L}_C$, étend donc le système $\mathscr{S}_C$.

N. B. On notera une *autre extension* de $\mathscr{S}_C$, d'ailleurs plus forte, extension qui correspond à l'énumération de toutes les fonctions définies en $\mathscr{S}_C$ ou encore à l'opération d'associer sa *valeur* à tout terme clos de $\mathscr{S}_C$. La preuve de la validité, en démontrant le caractère fonctionnel des règles associées aux $\bar{f}_n$, établit aussi que cette opération est une fonction combinatoire.

Conséquences pour le problème de Hilbert (plus exactement il s'agit de résoudre le problème de Hilbert pour *tout* système formel qui se présente dans la pratique mathématique).

Ce qu'on vient de dire montre que les principes de raisonnement formulés en $\mathscr{S}_C$ ne permettent pas de résoudre le problème de Hilbert concernant le système $\mathscr{S}_C$; de même, en gros, pour toute extension $\mathscr{S}$ de $\mathscr{S}_C$ qui est un système formel valide : c'est le théorème dit deuxième théorème d'incomplétude de Gödel (une formulation fine de ce théorème doit analyser la notion de système formel et par conséquent a besoin des notions de la théorie des fonctions récursives).

Le théorème de Gödel n'implique point une réponse négative au problème de Hilbert ; il reste à considérer l'hypothèse que, pour tout système formel $\mathscr{F}$ suggéré par la pratique (y compris la pratique ensembliste), on puisse trouver un système $\mathscr{S}_{\mathscr{F}}$ et une réalisation $\mathfrak{R}_{\mathscr{F}}$ pour laquelle $\mathscr{S}_{\mathscr{F}}$ soit valide, tels que $\neg\, \text{Dem}_{\mathscr{F}}\,(x, s^*)$ soit démontrable en $\mathscr{S}_{\mathscr{F}}$.

Certes, ceci suppose que pour tout $\mathscr{F}$ en question il existe une preuve combinatoire qui ne peut être formulée dans $\mathscr{F}$ au sens du § 0*a*) (iv). Mais, seule une analyse approfondie de la notion de preuve combinatoire peut exclure la possibilité envisagée : car, justement d'après ce même théorème d'incomplétude, pour *tout* $\mathscr{F}$ (non contradictoire) il existe des preuves *exactes* qui ne se formulent pas dans $\mathscr{F}$. Autrement dit, on ne peut exclure cette possibilité sans se servir d'une propriété des preuves combinatoires plus fine que, disons, leur validité au sens ensembliste.

Sans une analyse pareille on n'a que le résultat suivant : il n'existe aucun système formel $\mathscr{S}$ tel que :

(i) $\mathscr{S}$ permette de dériver formellement tout énoncé formulé dans $\mathscr{L}_C$ qui est valide dans $\mathfrak{R}_C$ (au sens combinatoire),

(ii) qu'on puisse établir la validité de $\mathscr{S}$ (dans $\mathfrak{R}_C$) au moyen d'un raisonnement combinatoire.

3. Développement de la théorie.

On va considérer l'hypothèse énoncée à la fin du § 2. D'après ce qu'on vient de dire, une solution *positive* du problème de Hilbert réclamerait une étude empirique (cf. A, § 1 concernant $X^{\mathscr{A}_s}$ et $D^{\mathscr{A}_s}$) de tous les systèmes formels que présente la pratique mathématique (d'où, d'ailleurs, l'intérêt pour le problème de Hilbert de trouver un seul système qui englobe la pratique).

Par contre une solution *négative* pourrait être obtenue de la façon suivante : on chercherait d'abord un système $\mathscr{S}$ qui satisfasse à la condition (i) (§ 2 fin) ; ensuite un système particulier $\mathscr{S}_1$ de la pratique tel que le problème de Hilbert concernant $\mathscr{S}_1$ ne puisse être résolu par les méthodes de $\mathscr{S}$.

On trouvera dans l'article sur la logique mathématique de : *Lectures on Modern Mathematics*, t. 3, ed. Saaty, (1965) un système $\mathscr{S}$ qui est censé satisfaire la condition (i) et, qui ne permet pas de démontrer la non-contradiction de l'Arithmétique du premier ordre [Chap. 3, Ex. 2]. L'idée de la construction du système $\mathscr{S}$ est que les preuves combinatoires peuvent être engendrées en *itérant* le type d'extension considérée p. 207 : le problème principal consiste évidemment à incorporer dans $\mathscr{S}$ *toutes* les itérations telles que chacune des démonstrations formelles admises ait une réalisation combinatoire. (D'après le § 2*d*) (ii) le système $\mathscr{S}$ tout entier n'a pas de réalisation combinatoire.)

On notera un parallélisme frappant avec A, § 3 : l'opération $\mathfrak{P}$ (former l'ensemble de toutes les parties d'un ensemble donné) est l'opération qui engendre l'échelle des types, et le problème principal est d'affirmer, sous forme d'un énoncé du langage ensembliste $\mathscr{L}_E$, l'existence d'autant d'itérations de cette opération que possible : autrement dit, de trouver des axiomes de l'infini qui expriment l'existence de types élevés.

N. B. Pour mieux comprendre la nature du problème de Hilbert, le lecteur pourrait le comparer au problème de la quadrature du cercle : (α) la formulation d'un système $\mathscr{S}$ satisfaisant (i) correspondrait à la caractérisation (mathématique) de la notion géométrique de construction au moyen de la règle et du compas, qui est que tout point ainsi constructible a des coordonnées pythagoréennes (c'est-à-dire exprimables par les opérations rationnelles et la racine carrée) ; (β) la preuve que $\neg\, \mathrm{Dem}_{\mathscr{S}_1}(x, s^*)$ n'est pas démontrable dans $\mathscr{S}$ correspondrait à la preuve que

$$\int_0^1 \sqrt{1 - x^2}\, dx$$

n'est pas pythagoréen. Les textes modernes, tout au moins ceux influencés par la doctrine formaliste, se passent souvent de l'étude de (α) qui fait intervenir une analyse axiomatique des notions géométriques,

ce qui n'a rien d'étonnant parce que la possibilité même d'une telle caractérisation est embarrassante pour cette doctrine ; voir l'introduction.

La comparaison en question conduit aussi au problème fort intéressant de l'édification d'une théorie de preuves qui soient effectivement intelligibles et non seulement valides ; en particulier, de preuves combinatoires intelligibles. Le problème géométrique correspondant serait de trouver une théorie des constructions faisables, ne faisant intervenir que des points « proches » aux points de départ, et stables pour des « petits » changements de données (ceci réclame évidemment la découverte de la métrique propre à l'intuition géométrique). Bien qu'une théorie des preuves intelligibles ne fasse pas partie de la logique au sens strict qui ne s'occupe que des questions de validité d'une sorte ou d'une autre, il se peut que cette théorie profite des *méthodes* de la théorie combinatoire des fondements.

Il ne reste plus qu'à dire quelques mots sur la conception intuitionniste (§ 2*a*)) de la pensée mathématique : cette conception dépasse la théorie combinatoire en ce qu'elle admet aussi des objets abstraits tels que les fonctions, fonctions de fonctions, etc. pourvu que ces objets ne fassent intervenir que des objets de la pensée mathématique ; en particulier, on n'admet toujours pas les notions ensemblistes dans leur sens réaliste. Il s'agit donc d'une théorie idéaliste. L'acceptation de ces *constructions abstraites* qui constitue le côté positif des mathématiques intuitionnistes, les distingue des mathématiques combinatoires.

N. B. Leur côté négatif, d'ailleurs mieux connu, consiste en une polémique contre les notions ensemblistes aussi peu convaincante que celle du réaliste borné contre l'idéaliste (« Quelle espèce d'animal est une preuve ? ») ou celle du formaliste contre les autres (« Où se trouvent les êtres abstraits ? »). Chacune de ces critiques est faible : elles oublient toutes qu'il y a plus de choses au ciel et sur la terre que ne le pense la philosophie (choisie au départ). Ceci ne diminue point l'intérêt des résultats positifs dans un cadre limité qui montrent, par exemple, que les objets acceptés suffisent pour une explication des phénomènes considérés.

Le problème de Hilbert peut être évidemment reformulé, les notions intuitionnistes remplaçant celles du § 2. Pour plus de détails, voir l'article 1*c*).

4. Résumé critique des Parties A et B.

Bref examen des résultats, en corrélation avec les considérations générales de l'introduction.

a) *Comparaison entre fondements ensemblistes et combinatoires.* — Tous deux

offrent une réponse à la question (en langage traditionnel de la logique) : que sont les mathématiques ? La réponse des premiers est un cas particulier de vues « réalistes », aussi met-elle l'accent sur les objets, non sur les raisonnements les touchant ; elle est que les mathématiques sont la théorie des *ensembles* (en un sens déterminé). Celle des seconds, un cas de vues « idéalistes », regarde les objets mathématiques abstraits comme façons de parler, et veut montrer que notre emploi de ces façons de parler est cohérent.

Cette réponse a ceci de remarquable qu'elle prétend, contrairement aux apparences, notre raisonnement mathématique « essentiellement » combinatoire ; essentiellement au sens logique (cf. B, § 3) que la *validité* de nos conclusions, dès que formulables combinatoirement, s'établit aussi combinatoirement.

L'unité ainsi conférée aux raisonnements mathématiques serait d'autant plus surprenante qu'elle les ramènerait tous à des mathématiques du type scolaire, puisque celles-ci sont des raisonnements combinatoires par excellence.

Les deux sortes de fondements séparent les problèmes mathématiques de toutes les questions ontologiques portant sur d'*autres* notions et objets abstraits que les fondements considérés. (En d'autres termes, la solution des problèmes mathématiques est rendue indépendante de l'existence, c'est-à-dire de l'objectivité de ces autres notions et objets.) Mais comme elles tracent la séparation de manière toute différente on ne saurait déduire du succès d'une séparation celui de l'autre.

Entre notions ensemblistes et structures intuitives classiques, la séparation résulte des conditions d'adéquation $E^{\mathscr{A}_S}$ et $U^{\mathscr{A}_S}$ (A, § 1*a*) : si $E^{\mathscr{A}_S}$ est vérifiée, une conclusion purement ensembliste (c'est-à-dire formulée dans $\mathscr{L}_E$ avec s. c. t. pour réalisation) découle aussi de principes ensemblistes — à savoir ceux utilisés pour dériver $E^{\mathscr{A}_S}$ — *dès* qu'elle découle des propriétés intuitives $\mathscr{A}_S$ de S ; si de plus $U^{\mathscr{A}_S}$ est vérifiée, cela vaut même dans le cas d'usage d'autres propriétés intuitives (formulées dans le même langage de S), pourvu que la conception intuitive S soit cohérente. (En la discussion du § 1*a* de B, il a déjà été précisé que dans le cadre ensembliste on ne peut pas formuler *pourquoi* les conditions d'adéquation sont correctes ; ainsi le problème d'obtenir ces conditions d'une façon rigoureuse appartient-il en propre aux fondements, bien qu'il ait été presque toujours résolu par des mathématiciens ; cf. fin de l'introduction.)

Dans les fondements combinatoires, on a, pour l'essentiel, les mêmes conclusions de séparations, avec les conditions d'adéquations de B, § 1*c* et B, § 1*d* à la place respectivement de $E^{\mathscr{A}_S}$ et $U^{\mathscr{A}_S}$.

On a vu, Partie A, § 1*a*) et § 2*a*), que les conditions d'adéquations sont satisfaites dans le cas des structures classiques, par exemple le cas de nos conceptions géométriques (continu), ou sur le hasard (probabilité) ; satisfaites en un sens plus faible pour les ordinaux ; non satisfaites dans l'état de nos connaissances par la notion (iii) du § 2*a*).

Par contre, dans les fondements combinatoires, la part des mathématiques jusqu'à présent séparée des notions ensemblistes s'avère congrue, bien que pas

du tout triviale, comme il est montré dans B, § 1*c*) ; et ne va pas au-delà de l'arithmétique du premier ordre au sens de l'exercice 2, chapitre 3, si l'on admet la caractérisation des preuves combinatoires mentionnée en B, § 3.

Il va sans dire que les deux fondements sont au mieux des auxiliaires pour l'étude des objets abstraits dont ils éliminent l'usage !

b) Les *fondements doctrinaires*, par définition, soutiennent leur réponse à la question : « Que sont les mathématiques ? », principalement en critiquant les notions de base des théories des fondements rivales ; en particulier, cela les autorise à ne pas reconnaître les défauts de leur position, quand même la formulation de ces défauts est impossible sans sortir des fondements visés. De tels défauts existent pour chacun des types de fondements [par exemple, dans le cas des fondements combinatoires, la non-définissabilité de la relation de conséquence au second ordre]. Cf. discussion du § 1, *a*), Partie B. (Il n'est donc pas surprenant qu'un intérêt pour les fondements combinatoires soit souvent associé avec une attitude critique envers les notions ensemblistes et d'ailleurs, un intérêt pour les fondements ensemblistes avec une critique de notions comme celles de propriété dans A, § 2*a* ou celle de construction intuitionniste dans B, § 3.)

Si l'on adopte ce point de vue doctrinaire, l'importance du théorème de Gödel (Th. 4, Partie A), est précisément que l'inadéquation des fondements combinatoires peut y être exprimée en termes combinatoires. Mais d'un point de vue moins légaliste, *une conception des fondements est défectueuse si elle n'a pas ses propres explications* (théoriques) *de faits expliqués par une autre conception*, l'un des buts des fondements, comme de toute théorie, étant d'élargir le domaine de compréhension théorique. De ce point de vue, le Théorème 5 de la Partie A constitue déjà un défaut des fondements combinatoires : on peut donner de bonnes raisons, en termes ensemblistes, pour le choix de règles formelles, alors qu'elles doivent être considérées comme données dans les fondements combinatoires (cf. discussion de B, § 1*a*)).

Un autre défaut (cf. dernier alinéa de B, § 2) est que, dans le cadre combinatoire, on ne peut définir le domaine des mathématiques combinatoires, alors qu'on peut au moins essayer, dans un cadre (constructif) élargi (cf. B, § 3).

Dans l'état présent des connaissances, il n'y a pas de notions permettant de résoudre ou même de formuler, la question correspondante pour l'ensemble des mathématiques : y a-t-il des notions suffisamment abstraites, et néanmoins précises, pour caractériser l'extension de l'ensemble des mathématiques ?

c) Le *formalisme grossier*, mentionné à la fin de l'introduction, est une glorieuse doctrine, qui a le bonheur de répondre à cette question. Cette doctrine n'accepte pas les notions de base combinatoires, et affirme que les mathématiques consistent en assertions de la forme : une configuration donnée concrètement a été construite en appliquant une règle mécanique donnée (avec la terminologie de la partie B, § 0 *b*) : seules les formules closes d'un langage combinatoire sont admises). Aucune affirmation générale sur ces configurations

n'appartenant aux mathématiques, les conditions d'adéquation minimales du § 1 *b* (problème de Hilbert de la non-contradiction) ne sont pas formulables, puisqu'elles comportent une variable x. Cette doctrine est certainement sans défaut au sens légaliste de *b*), simplement parce que ce qu'elle retient des mathématiques ne permet de formuler à peu près rien ! Evidemment ce culte de l'impuissance est basé sur la conviction qu'il n'y a pas d'explication (théorique) possible de propriétés fondamentales de l'expérience mathématique comme la validité des conséquences combinatoires des propriétés de concepts intuitifs abstraits (5).

Le lecteur est sans doute frappé de ce que dans cette doctrine l'essentiel des mathématiques réside dans les manipulations mécaniques, alors qu'il a appris à l'école qu'elles sont l'antithèse des mathématiques : « une démonstration ne s'apprend pas par cœur, il faut la comprendre ». (Et même, le lecteur se rappelle probablement que déjà il comprenait la différence entre les deux.)

La doctrine ne paraît donc pas très sensée ; par ailleurs elle contredit la pratique. Mais le plus sérieux reproche qu'elle encourt est d'avoir conduit certains à croire, ou au moins à affirmer l'impossibilité d'explications théoriques là où, en fait, on en dispose déjà, comme dans le cas particulier du programme de Hilbert décrit dans le § 1 *c* ; ce qui réfute déjà la thèse générale négative de la doctrine.

Les problèmes principaux des deux théories des fondements ici considérées sont la recherche de nouveaux axiomes (propriétés) des notions de base ensemblistes, c'est-à-dire de la s. c. t., respectivement l'analyse fine des notions de base combinatoires et la recherche des limites exactes du cadre combinatoire. En profitant de ces recherches, on développe de nouvelles théories.

On notera que les échecs du programme originel de Hilbert n'excluent pas la possibilité d'autres fondements « idéalistes », satisfaisant des conditions d'adéquations analogues à B, § 1*b*) ; cela est mentionné dans le § 3, qui contient une tentative dépassant le cadre proposé par Hilbert.

---

(5) Bourbaki flirte avec cette doctrine et propose une explication « empirique » invoquant l'expérimentation qu'ont subie les systèmes formels. Ceci n'est pas bien pesé ; l'on ne dit rien sur les principes (statistiques) pour évaluer cette expérimentation, et comme ceux-ci utiliseraient au moins les mathématiques combinatoires, l'on serait renvoyé à des problèmes très semblables à ceux de la partie B. En fait on peut sans doute appliquer ici les dernières lignes de la partie A.

C. COMPARAISON ENTRE L'INTRODUCTION SÉMANTIQUE ET L'INTRODUCTION SYNTAXIQUE (COMBINATOIRE) A LA LOGIQUE MATHÉMATIQUE

N. B. « Sémantique » signifie, comme il est d'usage, « sémantique ensembliste » ; bien que, dans l'analyse syntaxique, il faille aussi comprendre les notions de bases (combinatoires : celles de B, § 0).

1° L'analyse sémantique présente les avantages suivants :

a) D'après B, § 1*a*), et § 4, l'analyse syntaxique ou la théorie des démonstrations part de données fournies par l'analyse sémantique : le choix d'axiomes, de la relation de conséquence logique.

b) Certaines parties des mathématiques courantes qui *ont* un fondement sémantique reposant sur la s. c. t. (cf. A, § 2) n'ont pas de fondement combinatoire (cf. B, § 3) (et on n'en connaît pas de fondements constructifs).

[c) Plusieurs résultats de base du calcul des prédicats du premier ordre (classique) ont une formulation et une démonstration combinatoire, mais une démonstration utilisant le lemme 3 (complétude des règles) est plus facile. Cf. B, § 1*c*).

2° La faiblesse de l'analyse sémantique est que plusieurs résultats du § 1*c*) ci-dessus sont valables non seulement pour des règles sémantiquement complètes et correctes, mais aussi pour une vaste classe de règles, satisfaisant à des conditions formulées en termes combinatoires remarquablement simples, comme le lemme d'interpolation : l'analyse sémantique masque donc la *généralité* de ces résultats.]

Imprimé en France. — Imprimerie JOUVE, 12, rue de Tournon, PARIS (6e)
dépôt légal : N° 5248. — 4e trimestre 1966